

DO NOT REPRINT
© FORTINET



NSE 4 Immersion Solution Guide

for FortiOS 7.2

FORTINET®
Training Institute

DO NOT REPRINT

© FORTINET

Fortinet Training Institute - Library

<https://training.fortinet.com>

Fortinet Product Documentation

<https://docs.fortinet.com>

Fortinet Knowledge Base

<https://kb.fortinet.com>

Fortinet Fuse User Community

<https://fusecommunity.fortinet.com/home>

Fortinet Forums

<https://forum.fortinet.com>

Fortinet Product Support

<https://support.fortinet.com>

FortiGuard Labs

<https://www.fortiguard.com>

Fortinet Training Program Information

<https://www.fortinet.com/nse-training>

Fortinet | Pearson VUE

<https://home.pearsonvue.com/fortinet>

Fortinet Training Institute Helpdesk (training questions, comments, feedback)

<https://helpdesk.training.fortinet.com/support/home>

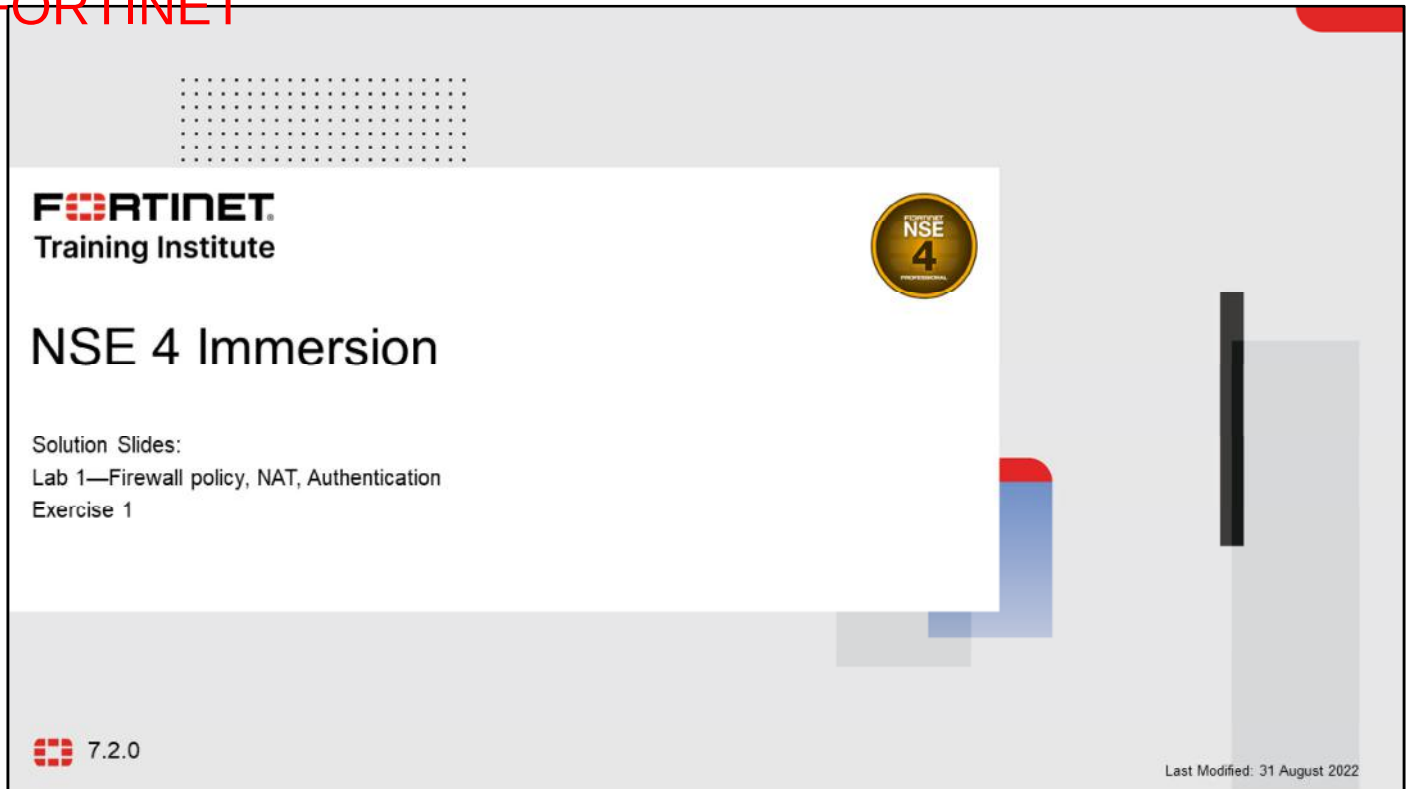


8/31/2022

TABLE OF CONTENTS

Solution - Lab 1 - Exercise 1.....	4
Solution - Lab 1 - Exercise 2.....	9
Solution - Lab 2 - Exercise 1.....	12
Solution - Lab 2 - Exercise 2.....	18
Solution - Lab 3 - Exercise 1.....	22
Solution - Lab 3 - Exercise 2.....	28
Solution - Lab 4 - Exercise 1.....	31
Solution - Lab 4 - Exercise 2.....	34
Solution - Lab 5 - Exercise 1.....	39
Solution - Lab 5 - Exercise 2.....	44
Solution - Lab 6 - Exercise 1.....	47
Solution - Lab 6 - Exercise 2.....	51
Solution - Lab 7 - Exercise 1.....	54
Solution - Lab 7 - Exercise 2.....	62

DO NOT REPRINT
© FORTINET



These slides contain the solutions to the labs.

DO NOT REPRINT
© FORTINET

Firewall Policy, DNAT, and Authentication—Part 1

- Requirement:
 - You must create a new firewall address object and firewall policy
- Solution:

Policy & Objects > Addresses

+ Create New
Address
Address Group

Name: LOCAL_SUBNET
Color: Change
Type: Subnet
IP/Netmask: 10.0.1.0 255.255.255.0
Interface: any
Static route configuration: ☐
Comments: Write a comment... 0/255

Policy & Objects > Firewall Policy

New Policy

Name: Internet_Access
Incoming Interface: port3
Outgoing Interface: port1
Source: LOCAL_SUBNET
Destination: all
Schedule: always
Service: ALL_ICMP, DNS, HTTP, HTTPS, SSH
Action: ACCEPT, DENY
Inspection Mode: Filter-based, Proxy-based
Firewall / Network Options:
NAT: ☐
IP Pool Configuration: Use Outgoing Interface Address, Use Dynamic IP Pool
Preserve Source Port: ☐
Logging Options:
Log Allowed Traffic: ☐
Generate Logs when Session Starts: ☐
Capture Packets: ☐
Comments: Write a comment... 0/1023
Enable this policy: ☐

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

2

- To create a firewall address object, navigate to **Policy & Objects > Addresses**, and then click **Create New > Address**.
- Enter `LOCAL_SUBNET` as the name of the address object and `10.0.1.0/24` as **IP/Netmask**.

A firewall policy can use the address object, created above.

Navigate to **Policy & Objects > Firewall Policy**, and then click **Create New** and use the following settings:

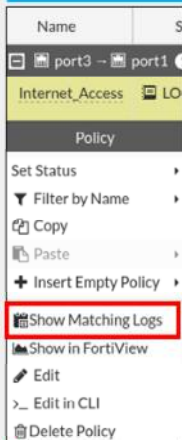
- **Name:** `Internet_Access`
- **Incoming Interface:** `port3`
- **Outgoing Interface:** `port1`
- **Source:** `LOCAL_SUBNET`
- **Destination:** `all`
- **Service:** `ALL_ICMP`, `HTTP`, `HTTPS`, `DNS`, `SSH`
- **Log Allowed Traffic:** `All Sessions`

DO NOT REPRINT
© FORTINET

Firewall Policy, DNAT, and Authentication—Part 2

- Requirement:
 - Display matching traffic logs after visiting a few websites on local client
- Solution:

Policy & Objects > Firewall Policy



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

3

Right-click **Internet_Access** firewall policy, and then click **Show Matching Logs**.

DO NOT REPRINT
© FORTINET

Firewall Policy, DNAT, and Authentication—Part 3

- Requirement:
 - You must create a new firewall policy to block ICMP traffic and reorder accordingly
- Solution:

Policy & Objects > Firewall Policy

New Policy

Name: Block_Ping

Incoming Interface: port3

Outgoing Interface: port1

Source: LOCAL_SUBNET

Destination: all

Schedule: always

Service: ALL_ICMP

Action: ☒ ACCEPT ☒ DENY

☒ Log Violation Traffic

Comments: Write a comment... 0/1023

Enable this policy ☒

Policy & Objects > Firewall Policy

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
1	Internet_Access	LOCAL_SUBNET	all	always	ALL_ICMP DNS HTTP HTTPS SSH	ACCEPT	Enabled	no-inspection	UTM	3.83 MB
2	Block_Ping	LOCAL_SUBNET	all	always	ALL_ICMP	DENY			All	0 B

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
2	Block_Ping	LOCAL_SUBNET	all	always	ALL_ICMP	DENY			All	0 B
1	Internet_Access	LOCAL_SUBNET	all	always	ALL_ICMP DNS HTTP HTTPS SSH	ACCEPT	Enabled	no-inspection	UTM	3.83 MB

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

4

Navigate to **Policy & Objects > Firewall Policy** and click **Create New** and use the following settings:

- Name:** Block_Ping
- Incoming Interface:** port3
- Outgoing Interface:** port1
- Source:** LOCAL_SUBNET
- Destination:** all
- Service:** ALL_ICMP
- Action:** DENY
- Log Violation Traffic:** enable

The new firewall policy appears below the **Internet_Access** firewall policy. You must reorder the policy to place it above the **Internet_Access** firewall policy.

DO NOT REPRINT
© FORTINET

Firewall Policy, DNAT, and Authentication—Part 4

- Requirement:
 - You must create a new VIP firewall object and place it on a firewall policy to allow inbound traffic
- Solution:

Policy & Objects > Virtual IPs

New Virtual IP

VIP type: IPv4

Name: VIP-INTERNAL-HOST

Comments: Write a comment... 0/255

Color: Change

Network

Interface: ☐ any

Type: ☒ Static NAT ☐ FQDN

External IP address/range: 10.200.1.200

Map to

IPv4 address/range: 10.0.1.10

New Policy

Name: Web-Server-Access

Incoming Interface: port1

Outgoing Interface: port3

Source: all

Destination: VIP-INTERNAL-HOST

Schedule: always

Service: HTTP, HTTPS

Action: ☒ ACCEPT ☐ DENY

Inspection Mode: ☒ Flow-based ☐ Proxy-based

Firewall / Network Options

NAT: ☐

Protocol Options: default

Logging Options

Log Allowed Traffic: ☒ Security Events ☒ All Sessions

Generate Logs when Session Starts: ☐

Capture Packets: ☐

Comments: Write a comment... 0/1023

Enable this policy: ☒

FORTINET
Training Institute

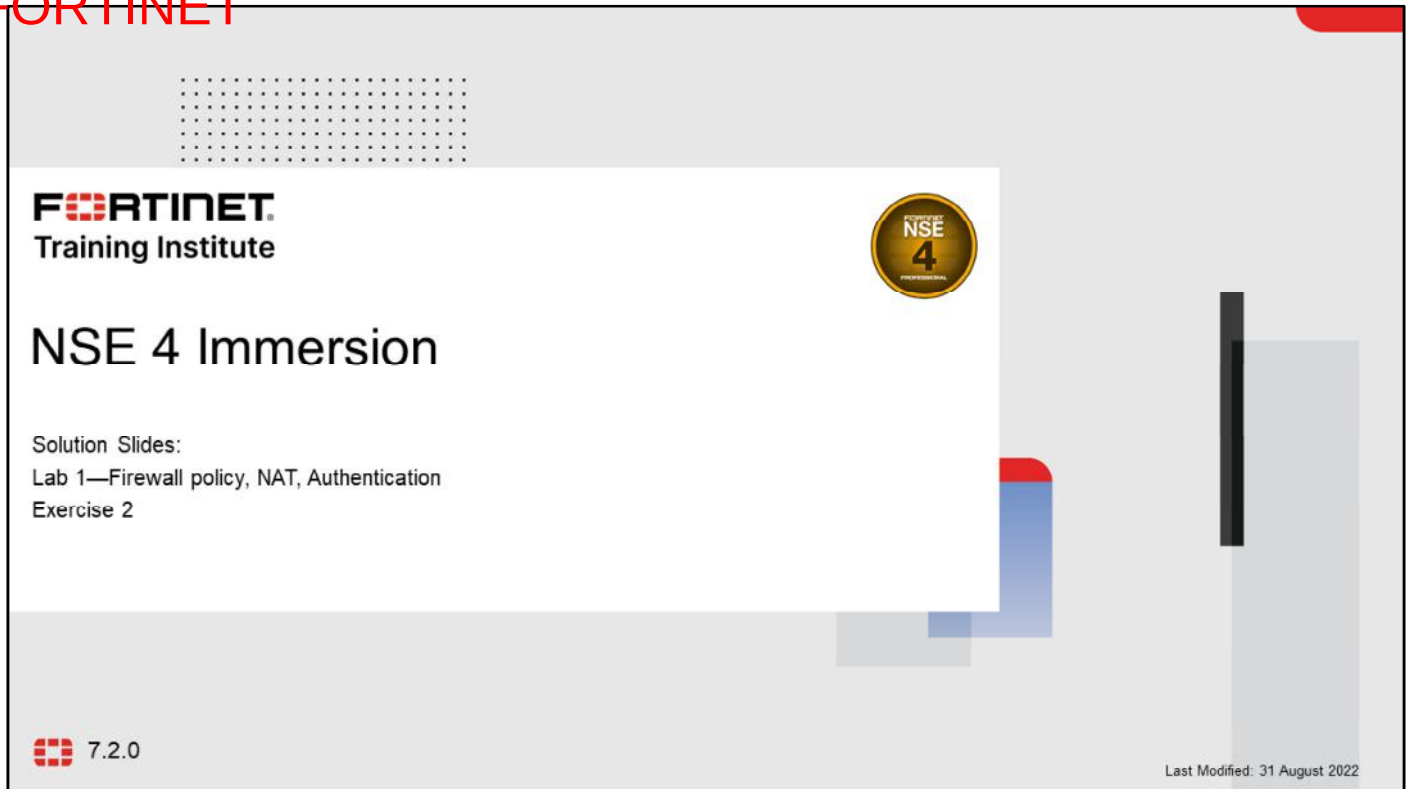
© Fortinet Inc. All Rights Reserved.

5

You must create a new VIP firewall object and place it on a firewall policy to allow inbound traffic.

- **Name:** Web-Server-Access
- **Incoming Interface:** port1
- **Outgoing Interface:** port3
- **Source:** all
- **Destination:** VIP-INTERNAL-HOST
- **Service:** HTTP, HTTPS
- **Log Allowed Traffic:** All Sessions

DO NOT REPRINT
© FORTINET



The slide features a light gray background with a white rectangular area on the left. At the top left of this white area is a grid of small dots. Below the grid is the Fortinet logo and the text "Training Institute". To the right of the logo is a gold circular badge with "NSE 4" and "PROFESSIONAL" inside. Below the logo and badge is the title "NSE 4 Immersion". Underneath the title is the text "Solution Slides:", "Lab 1—Firewall policy, NAT, Authentication", and "Exercise 2". At the bottom left of the white area is the Fortinet logo and the version number "7.2.0". At the bottom right of the slide is the text "Last Modified: 31 August 2022".

FORTINET
Training Institute

NSE 4 Immersion

Solution Slides:
Lab 1—Firewall policy, NAT, Authentication
Exercise 2

7.2.0

Last Modified: 31 August 2022

These slides contain the solutions to the labs.

DO NOT REPRINT
© FORTINET

Firewall Policy, DNAT, and Authentication—Part 5

- Requirement:
 - Assign an LDAP user group to a firewall user group and then to the firewall policy
- Solution:

User & Authentication > User Groups

Proxy-based profile

Policy & Object > Firewall Policy

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
2	Block_Ping	LOCAL_SUBNET	all	always	ALL ICMP	DENY			All
1	Internet_Access	LOCAL_SUBNET	all	always	ALL ICMP, HTTP, HTTPS, SSH	ACCEPT	Enabled	Web Filter: Category_Monitor, Certificate-Inspection	All

Dashboard > Users & Devices

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

2

- In the **Remote Server** drop-down list, select **External_Server**.
- On the **Groups** tab, right-click **AD-users**, and then click **Add Selected**.

The users in this AD group are now included in your FortiGate **Remote-users** firewall user group. Only users from the remote LDAP server that match this user group entry can authenticate.

- Configure **Internet_Access** firewall policy to include **Remote-users** group.
- In the **Inspection Mode**, select **Proxy-based**, because the webfilter profile (**Category_Monitor**) is configured as proxy-based.
- In the **Security Profiles** section, enable **Web Filter**, and then select **Category_Monitor**.

Monitor the firewall authenticated user. To view this login authentication:

- Click **Dashboard**, then select **Users & Devices**, and then click **Firewall Users** to expand it to full screen.
- Click **aduser1**, and then click **Deauthenticate**.

DO NOT REPRINT
© FORTINET

Firewall Policy, DNAT, and Authentication—Part 6

- Requirement:
 - Configure captive portal on the internal interface and assign a user group for authentication
- Solution:

Policy & Object > Firewall Policy

Name	Internet_Access
Incoming Interface	port3
Outgoing Interface	port1
Source	LOCAL_SUBNET Remote-users

User & Authentication > User Groups

New User Group

Name	CP-group
Type	Firewall
Members	student

Network > Interfaces

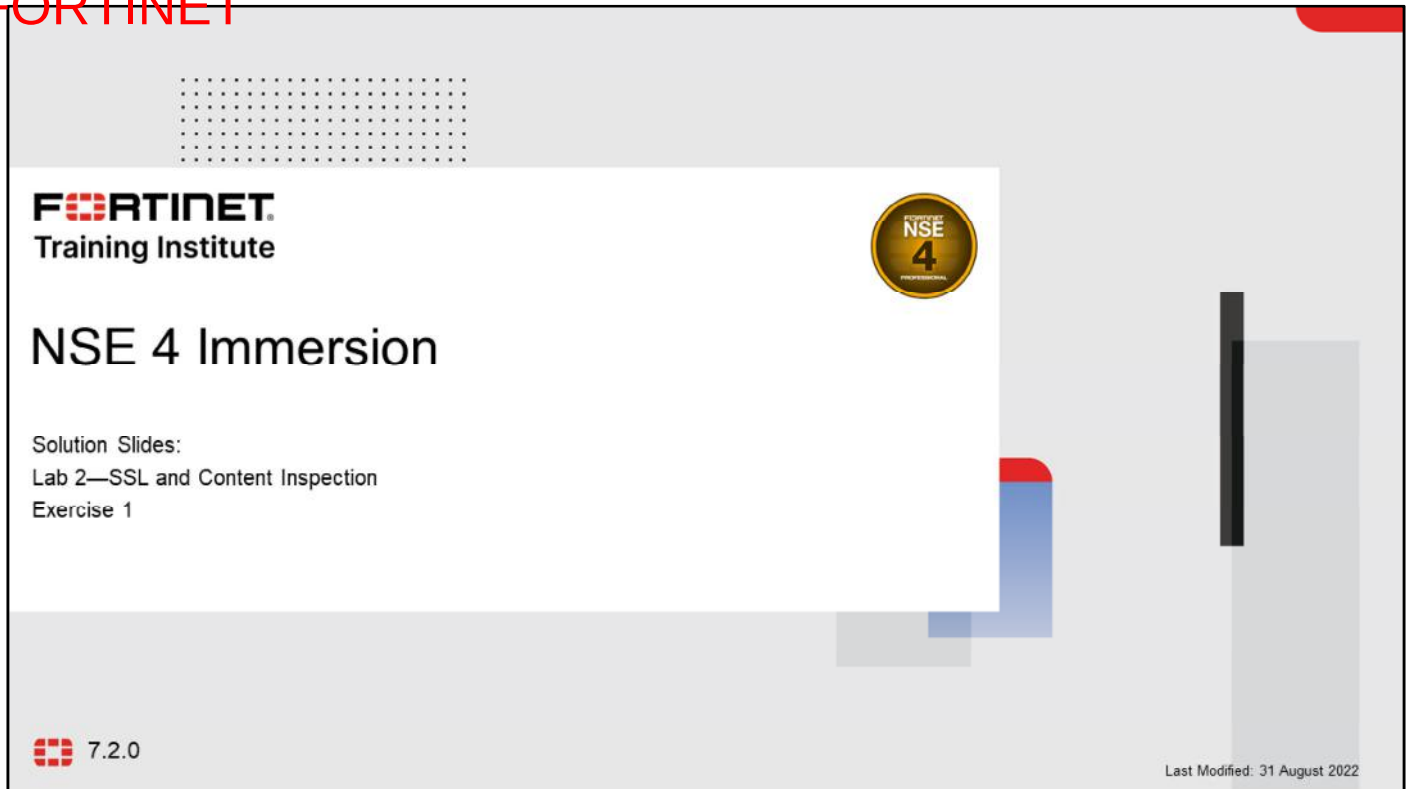
Network

Device detection	☒
Security mode	Captive Portal
Authentication portal	Local External
User access	Restricted to Groups Allow all
User groups	CP-group
Exempt sources	
Exempt destinations/services	
Redirect after Captive Portal	Original Request Specific URL

```
config firewall policy
edit 1
set disclaimer enable
next
end
```

Enable the disclaimer replacement message on the firewall policy ID 1

DO NOT REPRINT
© FORTINET



These slides contain the solutions to the labs.

DO NOT REPRINT
© FORTINET

SSL and Content Inspection—Full SSL Inspection

- Requirement:
 - Configure full SSL inspection profile and on firewall policy alongside web filter profile on Local-FortiGate
- Solution:

Security Profiles > SSL/SSH Inspection

New SSL/SSH Inspection Profile

Name: Custom_Full_Inspection

Comments: Write a comment... 0/255

SSL Inspection Options

Enable SSL inspection of: Multiple Clients Connecting to Multiple Servers

Protecting SSL Server

Inspection method: SSL Certificate Inspection Full SSL Inspection

Common Options

Invalid SSL certificates: Allow Block Custom

Log SSL anomalies: ☒

Policy & Object > Firewall Policy

Security Profiles

AntiVirus: ☐

Web Filter: ☒ WEB default

Video Filter: ☐

DNS Filter: ☐

Application Control: ☐

IPS: ☐

File Filter: ☐

SSL Inspection: ☒ SSL Custom_Full_Inspection

Decrypted Traffic Mirror: ☐

Logging Options

Log Allowed Traffic: ☒ Security Events All Sessions

Generate Logs when Session Starts: ☐

Capture Packets: ☐

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

2

DO NOT REPRINT
© FORTINET

SSL and Content Inspection—Web Filter

- Requirement:
 - Verify FortiGate settings and determine web filter categories
- Solution:

System > FortiGuard

Filtering	
Web Filter cache	☒ Clear cache after 60 Minutes
Email Filter cache	☒ Clear cache after 30 Minutes
FortiGuard filtering services	UDP 8888
Test Connectivity	
Filtering services availability	Web Filtering ☒ Anti-Spam ☒

www.fortiguards.com/webfilter

NEWS / RESEARCH SERVICES THREAT LOOKUP PSIRT RESOURCES

Home / Web Filter

Web Filter Lookup

www.twitter.com

Submit a URL to check its Rating

Category: Social Networking

7.0+ FortiOS Version

A social networking site is a platform to build social networks or social relations among people who share similar interests, activities, backgrounds or real-life connections. A social network service consists of a representation of each user (often a profile), his or her social links, and a variety of additional services. Social network sites are web-based services that allow individuals to create a public profile, create a list of users with whom to share connections, and view and cross the connections within the system.

Group: General Interest - Personal

At a glance:
Review the Web Filter Categories

WF Rating History

Nov 18, 2014 @ 13:10:07 PST
removed as Social Networking

Dec 02, 2014 @ 01:18:18 PST
removed as Social Networking

Dec 11, 2014 @ 07:50:06 PST
removed as Social Networking

Jan 08, 2014 @ 09:20:14 PST

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

3

Determine the web category for the following websites:

- www.twitter.com (Social Networking)
- www.skype.com (Internet Telephony)
- www.bing.com (Search Engines and Portals)
- www.dailymotion.com (Streaming Media and Download)

DO NOT REPRINT
© FORTINET

SSL and Content Inspection—Web Filter Category

- Requirement:
 - Configure web filter security profile to block URL on Local-FortiGate

- Solution: **Security Profiles > Web Filter**

Edit Web Filter Profile

Name: default

Comments: Default web filtering. 22/255

Feature set: **Flow-based** Proxy-based

FortiGuard Category Based Filter

Allow Monitor Block **Warning** Authenticate

Name	Action
Medicine	Allow
News and Media	Allow
Social Networking	Allow
Political Organizations	Monitor
Reference	Block

Cancel

FortiGuard Category Based Filter

Allow Monitor Block **Warning** Authenticate

Name	Action
Peer-to-peer File Sharing	Allow
Internet Radio and TV	Allow
Internet Telephony	Allow

Security Risk 6

Bandwidth Consuming

Freeview and Software Downloads	Allow
File Sharing and Storage	Allow
Streaming Media and Download	Allow
Peer-to-peer File Sharing	Allow
Internet Radio and TV	Allow
Internet Telephony	Warning

General Interest - Personal

Advertising	Allow
Web-based Email	Allow
News and Media	Allow
Social Networking	Allow
Political Organizations	Allow

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

4

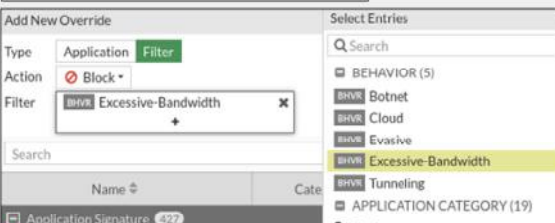
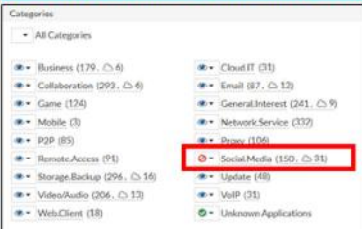
- Apply the actions to the URL categories and save the web filter profile.
- Enable the web-filter profile on the policy.
- Attempt to access the URLs and note the results.
- Modify the policy to allow www.twitter.com and www.dailymotion.com.

DO NOT REPRINT
© FORTINET

SSL and Content Inspection—Application Filter

- Requirement:
 - Configure an application filter override to block excessive bandwidth on Local-FortiGate
- Solution:

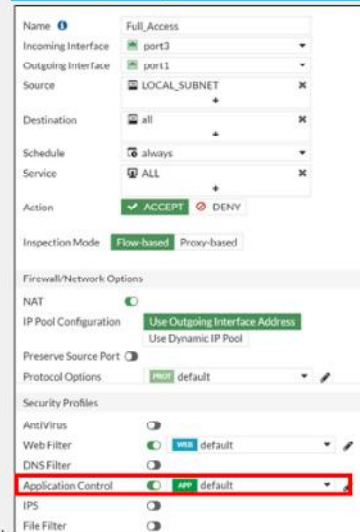
Security Profiles > Application Control



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

Policy & Object > Firewall Policy



5

- Configure an application control profile as a category and filter override to block applications.
- Enable application control profiles.
- Attempt to access the URLs and note the results.

DO NOT REPRINT
© FORTINET

SSL and Content Inspection—Application Signature

- Requirement:
 - Configure an application signature to allow Dailymotion on Local-FortiGate
- Solution:

Security Profiles > Application Control

Add New Override

Type: **Application** Filter

Action: **Allow**

Add All Results Remove Selected Dailymotion Selected All Cloud

Name	Category	Technology	Popularity	Risk
Application Signature 1/1737				
Dailymotion	Video/Audio	Browser-Based	★★★★★	

+ Create New Edit Delete

Priority	Details	Type	Action
1	Dailymotion	Application	Allow
2	Excessive-Bandwidth	Filter	Block

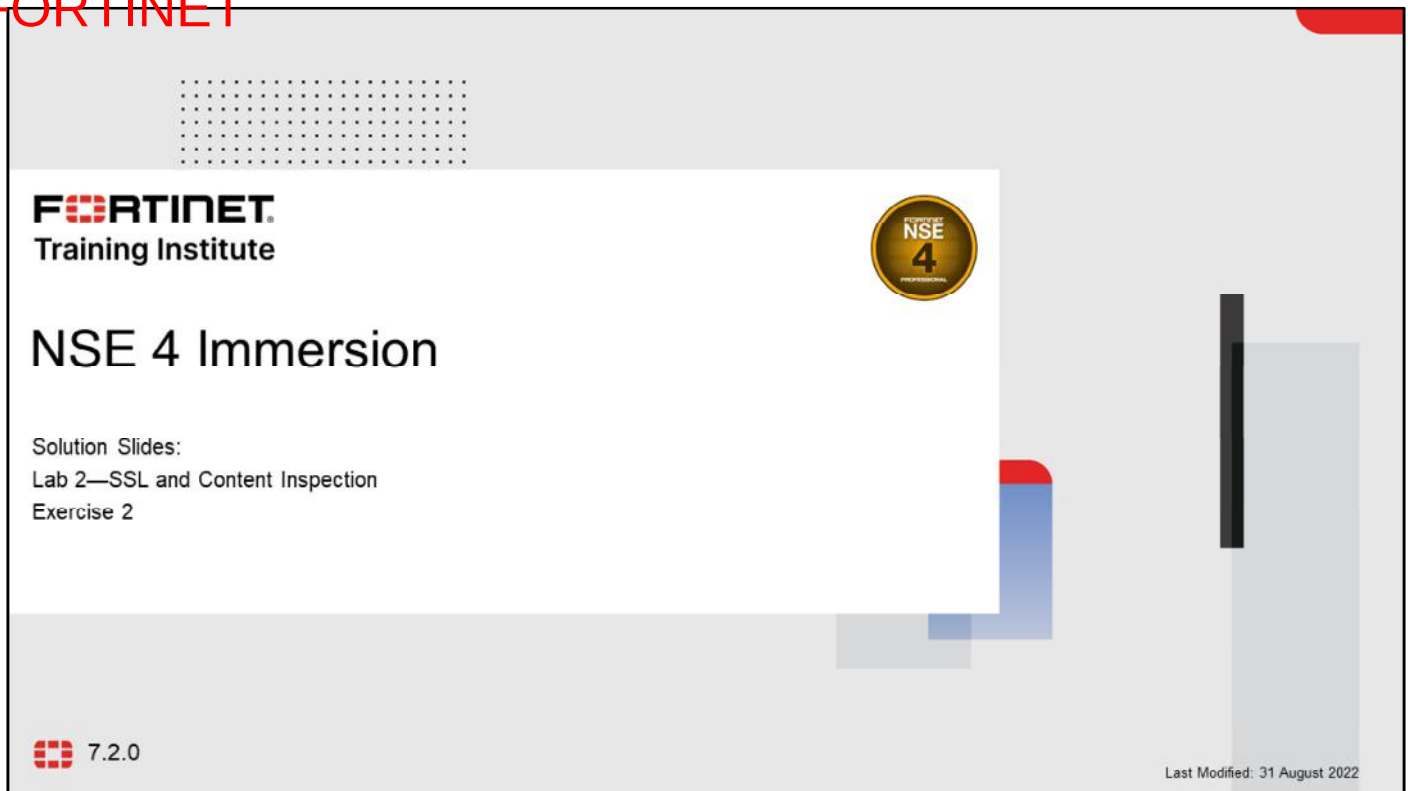
FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

6

Attempt to access www.dailymotion.com website in new browser window after an override.

DO NOT REPRINT
© FORTINET



These slides contain the solutions to the labs.

DO NOT REPRINT
© FORTINET

SSL and Content Inspection—Antivirus

- Requirement:
 - Verify the antivirus profile settings and enable profile on the firewall policy
- Solution:

Security Profiles > AntiVirus

Edit AntiVirus Profile

Name: default

Comments: Scan files and block viruses. 29/255

AntiVirus scan: ☒ Block ☐ Monitor

Feature set: ☒ Flow-based ☐ Proxy-based

Inspected Protocols:

☒ HTTP

☒ SMTP

☒ POP3

☒ IMAP

☒ FTP

☐ CIFS

Incoming Interface: port3

Outgoing Interface: port1

Source: LOCAL_SUBNET

Destination: all

Schedule: always

Service: ALL

Action: ☒ ACCEPT ☐ DENY

Inspection Mode: ☒ Flow-based ☐ Proxy-based

Firewall/Network Options

NAT: ☒

IP Pool Configuration: ☒ Use Outgoing Interface Address ☐ Use Dynamic IP Pool

Preserve Source Port: ☐

Protocol Options: ☐ default

Security Profiles

AntiVirus: ☒ default

Web Filter: ☐

DNS Filter: ☐

Application Control: ☐

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

2

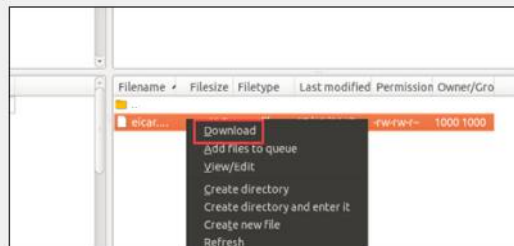
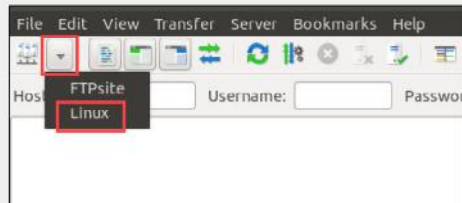
- Requirement:
 - Test the antivirus configuration by attempting to download files using HTTP
- Solution:



3

20

- Requirement:
 - Test the antivirus configuration by attempting to download files using FTP and review logs
- Solution:



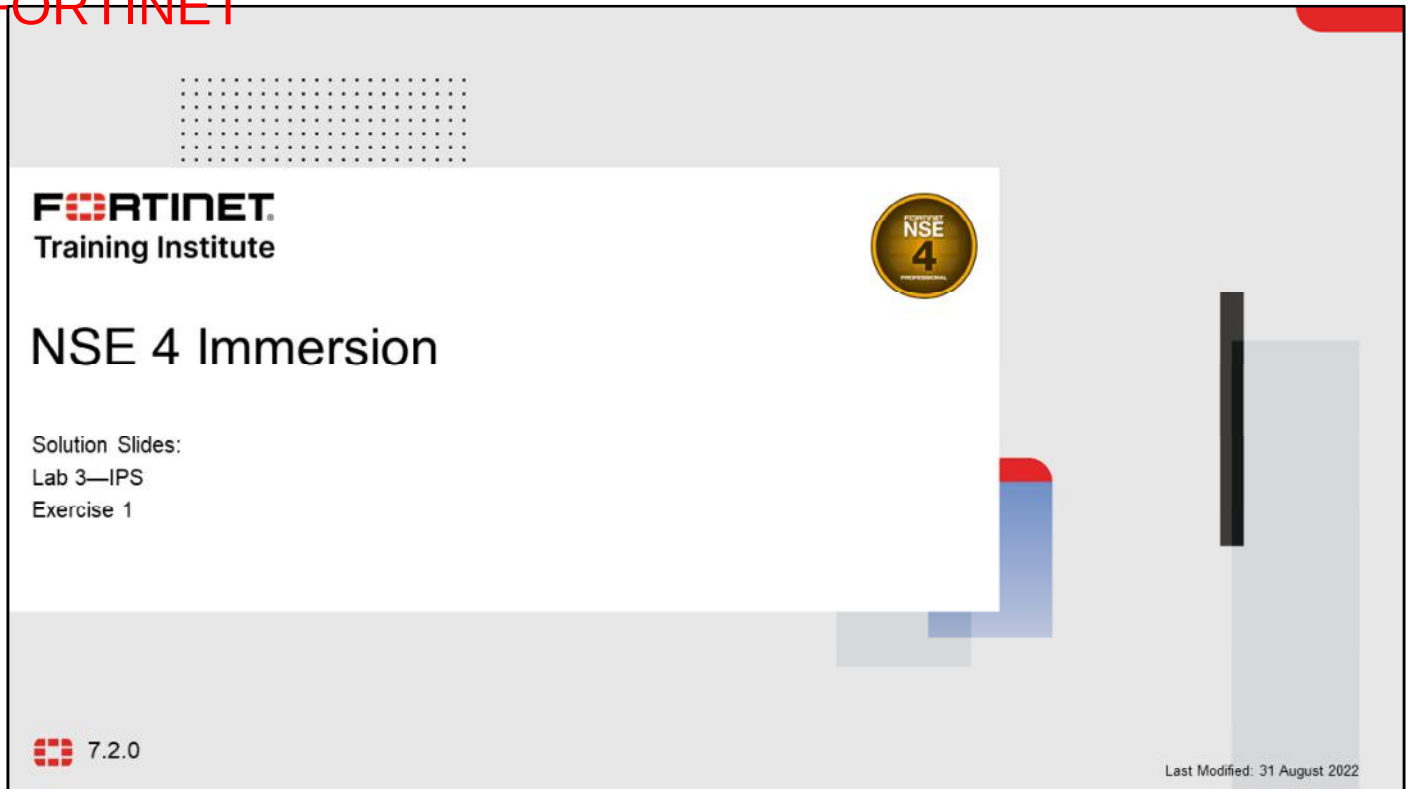
```
Command: RETReicar.com
Response: 150 Opening BINARY mode data connection for icar.com (68 bytes).
Error: Could not read from transfer socket: ECONNRESET - Connection reset by peer
Response: 226 Transfer complete.
Error: File transfer failed
```

Date/Time	%	Source	Destination	Application Name	Result	Log Details
12 seconds ago	10.0.1.10		10.200.1.254		Deny: UTM Blocked	Details General Absolute Date/Time: 2022/04/13 12:42:07 Time: 214:20:07 Duration: 5s Session ID: 12088 Virtual Domain: root Net Transition: Source
12 seconds ago	10.0.1.10		10.200.1.254		Deny: UTM Blocked	
2 seconds ago	10.0.1.10		10.200.1.254		Deny: UTM Blocked	
4 hours ago	10.0.1.10		10.200.1.254		Deny: UTM Blocked	
4 hours ago	10.0.1.10		10.200.1.254		✓ 800 B / 2.38 kb	
4 hours ago	10.0.1.10		10.200.1.254		✓ UTM Allowed	
4 hours ago	10.0.1.10		10.200.1.254		✓ 1.15 kb / 1.91 kb	
4 hours ago	10.0.1.10		10.200.1.254		Deny: UTM Blocked	Source IP: 10.0.1.10 NAT IP: 10.200.1.1 Source Port: 40391 NAT Port: 80429 Country/Region: Reserved Source Interface: port3 User:
4 hours ago	10.0.1.10		10.200.1.254		Deny: UTM Blocked	
4 hours ago	10.0.1.10		10.200.1.254		Deny: UTM Blocked	Destination IP: 10.200.1.254 Port: 7430 Country/Region: Reserved Destination Interface: port1
1 day ago	10.0.1.200	10.200.1.112.53			✓ 2.41 kb / 9.07 kb	
1 day ago	10.0.1.200	10.200.1.112.53			✓ 2.27 kb / 7.94 kb	
1 day ago	10.0.1.200	10.200.1.112.53			✓ 2.13 kb / 8.27 kb	
1 day ago	10.0.1.200	10.200.1.112.53			✓ 2.00 kb / 7.27 kb	

Date/Time	%	Service	Source	File Name	Virus/Botnet	User	Details	Action
3 minutes ago		FTP	10.0.1.10	icar.com	ICAR_TEST_FILE		Host: 10.200.1.254	Blocked
5 minutes ago		FTP	10.0.1.10	icar.com	ICAR_TEST_FILE		Host: 10.200.1.254	Blocked
5 minutes ago		FTP	10.0.1.10	icar.com	ICAR_TEST_FILE		Host: 10.200.1.254	Blocked
45 minutes ago		HTTPS	10.0.1.10	icar.com	ICAR_TEST_FILE		URL: https://secure.icar.org/icar.com	Blocked

Attempt to download the infected file using FTP. Review the log entries for the traffic and security profile.

DO NOT REPRINT
© FORTINET



These slides contain the solutions to the labs.

DO NOT REPRINT
© FORTINET

Block Known Exploits

- Requirement:
 - Configure IPS inspection profile
- Solution:

Security Profiles > Intrusion Prevention

New IPS Sensor

Name

Comments 0/255

Block malicious URLs ☐

IPS Signatures and Filters

[+ Create New](#) [Edit](#) [Delete](#)

Details	Exempt IPs	Action	Packet Logging
No results			

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

2

DO NOT REPRINT
© FORTINET

Block Known Exploits—IPS Filter

IPS Signatures and Filters

The image displays three sequential screenshots of the Fortinet IPS Signatures and Filters configuration page, illustrating the steps to add filters for different severity levels.

- Top Screenshot:** The 'Add Signatures' section shows 'Filter' selected as the Type. The 'Action' is set to 'Default'. The 'Status' is 'Enable'. The 'Filter' field is empty. The 'Select Entries' section shows a search for 'medium' and one result, 'SEVERITY (1)', with a severity level of 'MEDIUM'.
- Middle Screenshot:** The 'Filter' field now contains 'SEV'. The 'Select Entries' section shows a search for 'high' and one result, 'SEVERITY (1)', with a severity level of 'HIGH'.
- Bottom Screenshot:** The 'Filter' field now contains 'SEV'. The 'Select Entries' section shows a search for 'Critical' and one result, 'SEVERITY (1)', with a severity level of 'CRITICAL'.

Add medium, high, and critical filters

DO NOT REPRINT
© FORTINET

Block Known Exploits—Firewall Policy

- Requirement:
 - Apply an IPS sensor to a VIP firewall policy
- Solution:

Policy & Objects > Virtual IPs

New Virtual IP

VIP type: IPv4

Name: **VIP-WEB-SERVER**

Comments: Write a comment... 0/255

Color: Change

Network

Interface: **port1**

Type: **Static NAT** **FQDN**

External IP address/range: 10.200.1.200

Map to

IPv4 address/range: 10.0.1.10

Policy & Objects > Firewall Policy

New Policy

Name: **Web_Server_Access_IPS**

Incoming Interface: **port1**

Outgoing Interface: **port3**

Source: **all**

Destination: **VIP-WEB-SERVER**

Schedule: **always**

Service: **ALL**

Action: **ACCEPT** **DENY**

Inspection Mode: **Flow-based** **Proxy-based**

Firewall / Network Options

NAT: ☒

Protocol Options: **PROT** default

Security Profiles

AntiVirus: ☐

Web Filter: ☐

DNS Filter: ☐

Application Control: ☐

IPS: ☒ **IP** **WEBSERVER**

File Filter: ☐

SSL Inspection: **SSL** **certificate-inspection**

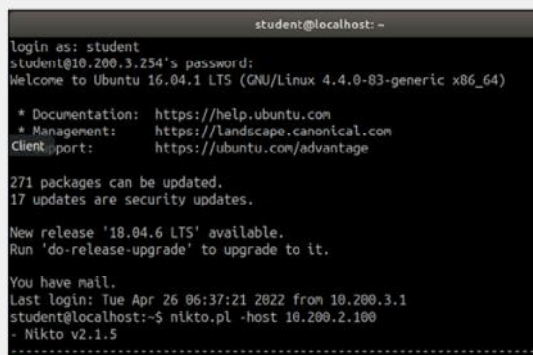
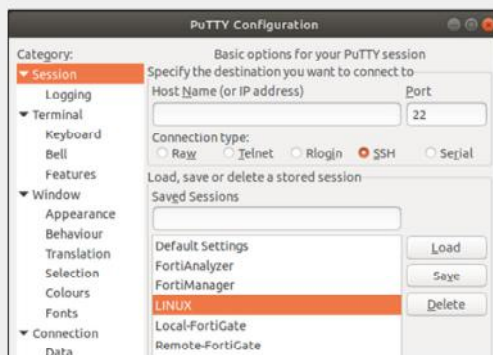
FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

4

Block Known Exploits—Generate Attack

- Requirement:
 - Generate attack from the Linux server



- On the Local-Client VM, open PuTTY, and then connect over SSH to the **LINUX** saved session.
- Log in with the username `student` and password `password`.
- Run the following script to start the attacks:
`nikto.pl -host 10.200.1.200`
- Leave the PuTTY session open (you can minimize it) so traffic continues to generate.

DO NOT REPRINT
© FORTINET

Block Known Exploits—Monitor IPS Logs

- Requirement:
 - Locate and review the IPS logs for all detected and dropped attacks
- Solution: **Log & Reports > Security Events > Intrusion Prevention**

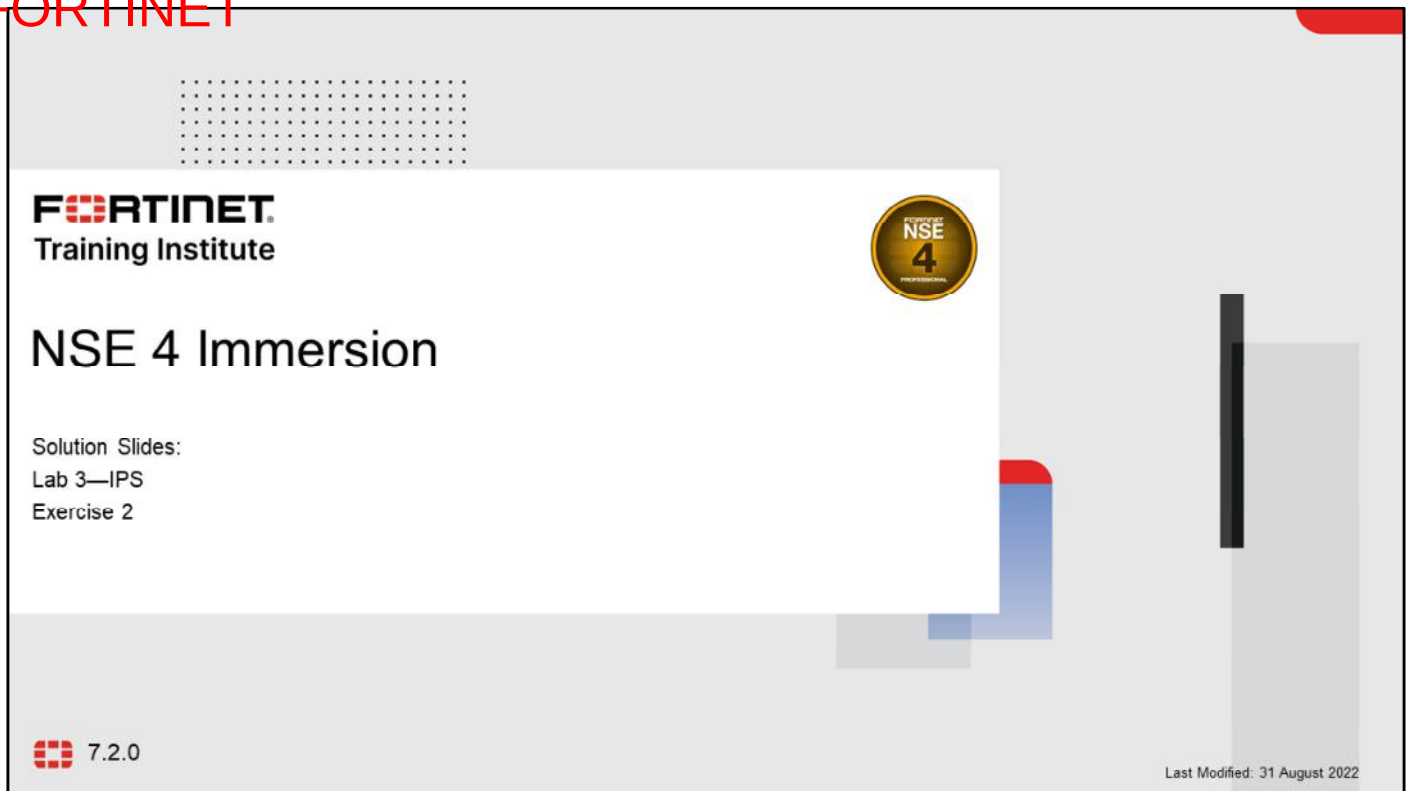
Summary										Details	
Date/Time	%	Severity	Source	Protocol	User	Action	Count	Attack Name		Log Details	
10 minutes ago		High	10.200.1.254	6		dropped		Mazens/PHPChat/Multiple File Inclusion		Policy Type	Firewall
10 minutes ago		High	10.200.1.254	6		dropped		Mazens/PHPChat/Multiple File Inclusion		Security	
10 minutes ago		High	10.200.1.254	6		dropped		AnyInventory.Environment/PHPFile.Inclusion		Level	High
10 minutes ago		High	10.200.1.254	6		dropped		AnyInventory.Environment/PHPFile.Inclusion		Threat Level	Medium
11 minutes ago		High	10.200.1.254	6		dropped		DFD/CarSet.Depth.Parameter/File.Inclusion		Threat Score	30
11 minutes ago		High	10.200.1.254	6		dropped		DFD/CarSet.Depth.Parameter/File.Inclusion		Cellular	
11 minutes ago		High	10.200.1.254	6		dropped		DFD/CarSet.Depth.Parameter/File.Inclusion		Service	HTTP
11 minutes ago		High	10.200.1.254	6		dropped		DFD/CarSet.Depth.Parameter/File.Inclusion		Other	
11 minutes ago		High	10.200.1.254	6		dropped		DFD/CarSet.Depth.Parameter/File.Inclusion		Log event original	1650510561949946400
11 minutes ago		High	10.200.1.254	6		dropped		DFD/CarSet.Depth.Parameter/File.Inclusion		Timestamp	-0700
12 minutes ago		High	10.200.1.254	6		dropped		DFD/CarSet.Depth.Parameter/File.Inclusion		Log ID	0419016384
12 minutes ago		High	10.200.1.254	6		dropped		DFD/CarSet.Depth.Parameter/File.Inclusion		Type	vpn
12 minutes ago		High	10.200.1.254	6		dropped		DFD/CarSet.Depth.Parameter/File.Inclusion		Sub Type	ips
12 minutes ago		High	10.200.1.254	6		detected		Ajax/File/Browser/approot/Parameter/File.Inclusion		Event Type	signature
12 minutes ago		High	10.200.1.254	6		detected		Ajax/File/Browser/approot/Parameter/File.Inclusion		Severity	High
12 minutes ago		High	10.200.1.254	6		dropped		Somery/Include/PHPFile.Inclusion		Source	undefined
12 minutes ago		High	10.200.1.254	6		dropped		Somery/Include/PHPFile.Inclusion		Interface	undefined
12 minutes ago		High	10.200.1.254	6		dropped		Somery/Include/PHPFile.Inclusion		Rule	undefined
12 minutes ago		High	10.200.1.254	6		dropped		Somery/Include/PHPFile.Inclusion		Destination	undefined
12 minutes ago		High	10.200.1.254	6		detected		RipeCMS/Parameter/Level/File.Inclusion		Attack Name	AnyInventory.Environment/PHPFile.Inclusion
12 minutes ago		High	10.200.1.254	6		detected		RipeCMS/Parameter/Level/File.Inclusion		HTTP	
12 minutes ago		High	10.200.1.254	6		detected		Ajax/File/Browser/approot/Parameter/File.Inclusion		request method	GET
12 minutes ago		High	10.200.1.254	6		dropped		NuclearBB/Root_Path/Parameter/File.Inclusion		Direction	outgoing
13 minutes ago		High	10.200.1.254	6		dropped		NuclearBB/Root_Path/Parameter/File.Inclusion		Attack ID	15100
13 minutes ago		High	10.200.1.254	6		dropped		NuclearBB/Root_Path/Parameter/File.Inclusion		Profile	default
13 minutes ago		High	10.200.1.254	6		dropped		NuclearBB/Root_Path/Parameter/File.Inclusion		Reference	http://www.fortinet.com/ids/VID15100
13 minutes ago		High	10.200.1.254	6		dropped		NuclearBB/Root_Path/Parameter/File.Inclusion		Incident	250609734
13 minutes ago		High	10.200.1.254	6		dropped		NuclearBB/Root_Path/Parameter/File.Inclusion		Serial No.	250609734

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

6

DO NOT REPRINT
© FORTINET

A presentation slide with a light gray background. At the top left, there is a grid of small dots. Below it, the Fortinet logo is displayed in red and black, followed by "Training Institute" in black. To the right of the logo is a gold circular badge with "NSE 4" and "PROFESSIONAL" text. The main title "NSE 4 Immersion" is in large black font. Below the title, the text "Solution Slides:", "Lab 3—IPS", and "Exercise 2" are listed. In the bottom left corner, the Fortinet logo is followed by "7.2.0". In the bottom right corner, the text "Last Modified: 31 August 2022" is present. The slide features abstract geometric shapes in blue and red on the right side.

FORTINET
Training Institute

NSE 4
PROFESSIONAL

NSE 4 Immersion

Solution Slides:
Lab 3—IPS
Exercise 2

7.2.0

Last Modified: 31 August 2022

These slides contain the solutions to the labs.

Mitigate DoS Attack—DoS Policy

- Requirement:
 - Create a DoS policy
- Solution:

Policy & Objects > IPv4 DoS Policy

New Policy

Name	ICMP_Floods
Incoming Interface	port1
Source Address	all
Destination Address	all
Service	ALL

L4 Anomalies

Name	Logging	Action			Threshold
		Disable	Block	Monitor	
tcp_syn_flood	☐	Disable	Block	Monitor	2000
tcp_port_scan	☐	Disable	Block	Monitor	1000
tcp_src_session	☐	Disable	Block	Monitor	5000
tcp_dst_session	☐	Disable	Block	Monitor	5000
udp_flood	☐	Disable	Block	Monitor	2000
udp_scan	☐	Disable	Block	Monitor	2000
udp_src_session	☐	Disable	Block	Monitor	5000
udp_dst_session	☐	Disable	Block	Monitor	5000
icmp_flood	☒	Disable	Block	Monitor	200
icmp_sweep	☐	Disable	Block	Monitor	100

DO NOT REPRINT
© FORTINET

Test DoS Policy & Examine Logs

- Requirement:
 - Generate an ICMP flood
 - Solution:
- Requirement:
 - Examine the logs
 - Solutions:

```
student@localhost: ~
login as: student
student@10.200.3.254's password:
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-83-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

271 packages can be updated.
17 updates are security updates.

New release '16.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

You have mail.
Last login: Tue Apr 26 06:42:17 2022 from 10.200.3.1
student@localhost:~$ sudo ping -f 10.200.1.1
[sudo] password for student:
PING 10.200.1.1 (10.200.1.1) 56(84) bytes of data.
```

Log & Reports > Security Events > Anomaly

Date/Time	Severity	Source	Protocol	User	Action	Count	Attack Name	Log Details
10 seconds ago	CRITICAL	10.200.1.254	ICMP		clear_session	2,389	icmp_flood	IP Destination Interface 10.200.1.1
40 seconds ago	CRITICAL	10.200.1.254	ICMP		clear_session	2,385	icmp_flood	Application Control Protocol 1 Service PING
Minute ago	CRITICAL	10.200.1.254	ICMP		clear_session	1	icmp_flood	Action clear_session Threat 4096 Policy ID ICMP_Floods(1) Policy Type DoS (IPv4)

Security
Level
Threat Level
Threat Score 50

Collector
Service PING

Anomaly
Attack Name
icmp_flood
Attack ID 18777218
ICMP ID 0x375a
ICMP Type 0x08

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

3

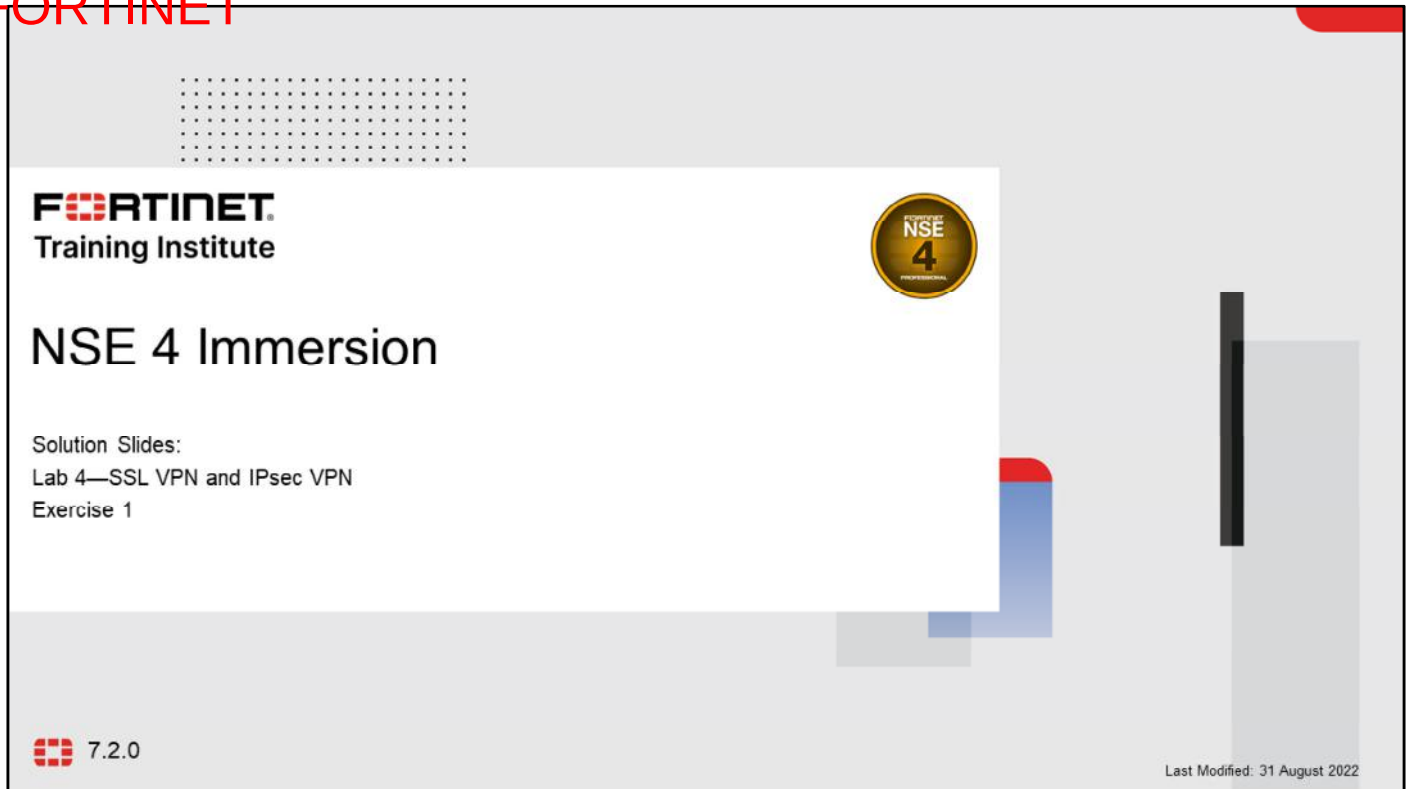
To test DoS policy:

- On the Local-Client VM, open PuTTY, and then connect over SSH to the **LINUX** saved session.
- Log in with the username `student` and password `password`.
- Enter the following command to generate an ICMP flood to the Local-FortiGate:

```
sudo ping -f 10.200.1.1
```

 A password prompt for the student account is displayed.
- Enter `password`. For every ping sent, the SSH session displays a period.
- Leave the SSH connection open with the ping running (you can minimize the window).

DO NOT REPRINT
© FORTINET



These slides contain the solutions to the labs.

DO NOT REPRINT
© FORTINET

SSL VPN Settings

- Requirement:
 - Configure SSL VPN web mode settings on Local-FortiGate
- Solution:

User & Authentication > User Definition

Users/Groups Creation Wizard

1 User Type > 2 Login Credentials > 3 Contact Info > 4 Extra Info

Username: student

Password: *****

Users/Groups Creation Wizard

1 User Type > 2 Login Credentials > 3 Contact Info > 4 Extra Info

User Account Status: ☒ Enabled ☐ Disabled

User Group: ☒ SSL_VPN_USERS ☐ +

VPN > SSL-VPN Settings

Connection Settings

Enable SSL-VPN: ☒

Listen on Interface(s): port1

Listen on Port: 10443

Web mode access will be listening at <https://10.200.1.1:10443>

Server Certificate: Fortinet_Factory

Redirect HTTP to SSL-VPN: ☒

Restrict Access: ☒ Allow access from any host ☐ Limit access to specific hosts

Idle Logout: ☒

Inactive For: 3000 Seconds

Authentication/Portal Mapping

+ Create New Edit Delete Send SSL-VPN Configuration

Users/Groups	Portal
All Other Users/Groups	web-access

DO NOT REPRINT
© FORTINET

SSL VPN Firewall Policy

- Requirement:
 - Configure SSL VPN firewall policy on Local-FortiGate and access SSL VPN portal
- Solution:

Policy & Object > Firewall Policy

New Policy

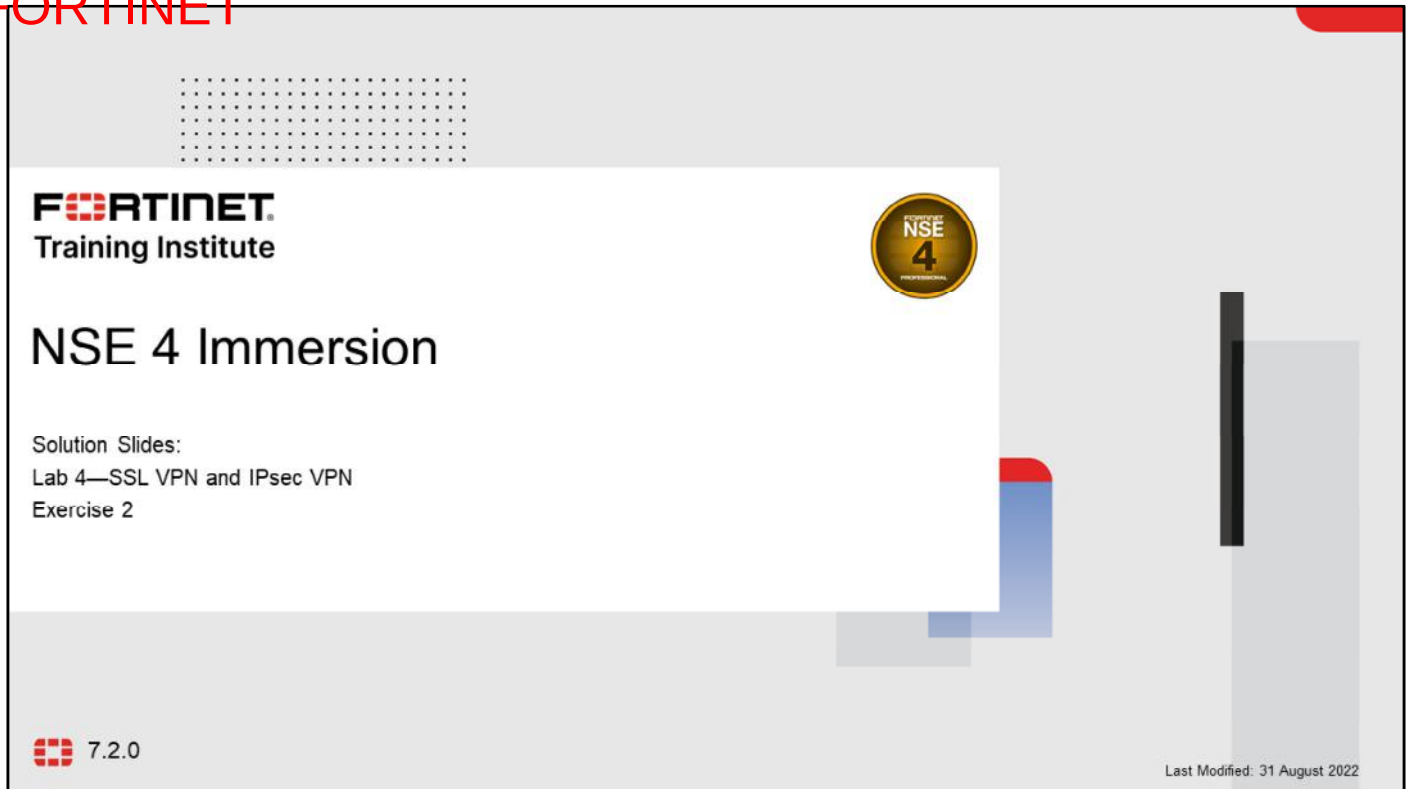
Name	SSL-VPN-Access
Incoming Interface	SSL-VPN tunnel interface (sslroot)
Outgoing Interface	port3
Source	SSLVPN_TUNNEL_ADDR1 SSL_VPN_USERS
Destination	LOCAL_FORTINET
Schedule	always
Service	ALL
Action	☒ ACCEPT ☐ DENY
Inspection Mode	Flow-based Proxy-based
Firewall / Network Options	NAT ☐

< Quick Connection

HTTP/HTTPS	FTP	RDP
	SMB/CIFS	VNC
	SFTP	
Host	10.0.1.10	
Port	3389	
Use SSL-VPN Credentials	☐	
Username	Administrator	
Password	*****	

Quick connection to establish SSL VPN to Local-FortiGate

DO NOT REPRINT
© FORTINET



These slides contain the solutions to the labs.

DO NOT REPRINT
© FORTINET

IPsec VPN—Site-to-Site IPsec—Local

- Requirement:
 - Configure site-to-site IPsec VPN tunnel and static route on Local-FortiGate
- Solution:

VPN > IPsec Tunnels

Network

IP Version: IPv4

Remote Gateway: Static IP Address

IP Address: 10.200.3.1

Interface: port1

Local Gateway: ☒

Mode Config: ☐

NAT Traversal: ☒ Enable ☐ Disable ☐ Forced

Keepalive Frequency: 10

Dead Peer Detection: ☐ Disable ☒ On Idle ☐ On Demand

DPD retry count: 3

DPD retry interval: 20 s

Forward Error Correction: Egress ☐ Ingress ☐

☒ Advanced...

Phase 2 Selectors

Name	Local Address	Remote Address
ToRemote	10.0.1.0/24	10.0.2.0/24

Edit Phase 2

Name: ToRemote

Comments: Comments

Local Address: Subnet 10.0.1.0/24

Remote Address: Subnet 10.0.2.0/24

Network > Static Routes

New Static Route

Destination: Subnet 10.0.2.0/24

Interface: ToRemote

Administrative Distance: 10

Comments: Write a comment... 0/255

Status: ☒ Enabled ☐ Disabled

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

2

DO NOT REPRINT
© FORTINET

IPsec VPN—Firewall Policy—Local

- Requirement:
 - Configure firewall policies for VPN traffic on Local-FortiGate
- Solution:

Policy & Object > Firewall Policy

Name	Source	Destination	Schedule	Service	Action	NAT
port3 → port1 1	port3	port1				
port3 → ToRemote 1	port3	ToRemote				
Remote_out	LOCAL_SUBNET	REMOTE_SUBNET	always	ALL	✓ ACCEPT	✗ Disabled
ToRemote → port3 1	ToRemote	port3				
Remote_in	REMOTE_SUBNET	LOCAL_SUBNET	always	ALL	✓ ACCEPT	✗ Disabled

DO NOT REPRINT
© FORTINET

IPsec VPN—Site-to-Site IPsec—Remote

- Requirement:
 - Configure site-to-site IPsec VPN tunnel and static route on Remote-FortiGate
- Solution:

VPN > IPsec Tunnels

Network

IP Version: **IPv4** | IPv6

Remote Gateway: Static IP Address

IP Address: 10.200.1.1

Interface: port4

Local Gateway: ☐

Mode Config: ☐

NAT Traversal: **Enable** | Disable | Forced

Keepalive Frequency: 10

Dead Peer Detection: **Disable** | On Idle | On Demand

DPD retry count: 3

DPD retry interval: 20 s

Forward Error Correction: Egress ☐ Ingress ☐

Advanced...

Phase 2 Selectors

Name	Local Address	Remote Address
Tolocal	10.0.2.0/24	10.0.1.0/24

New Phase 2

Name: Tolocal

Comments: Comments

Local Address: Subnet | 10.0.2.0/24

Remote Address: Subnet | 10.0.1.0/24

Network > Static Routes

Edit Static Route

Destination: **Subnet** | Internet Service

10.0.1.0/24

Interface: **ToLocal**

Administrative Distance: 10

Comments: Write a comment... 0/255

Status: **Enabled** | Disabled

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

4

DO NOT REPRINT
© FORTINET

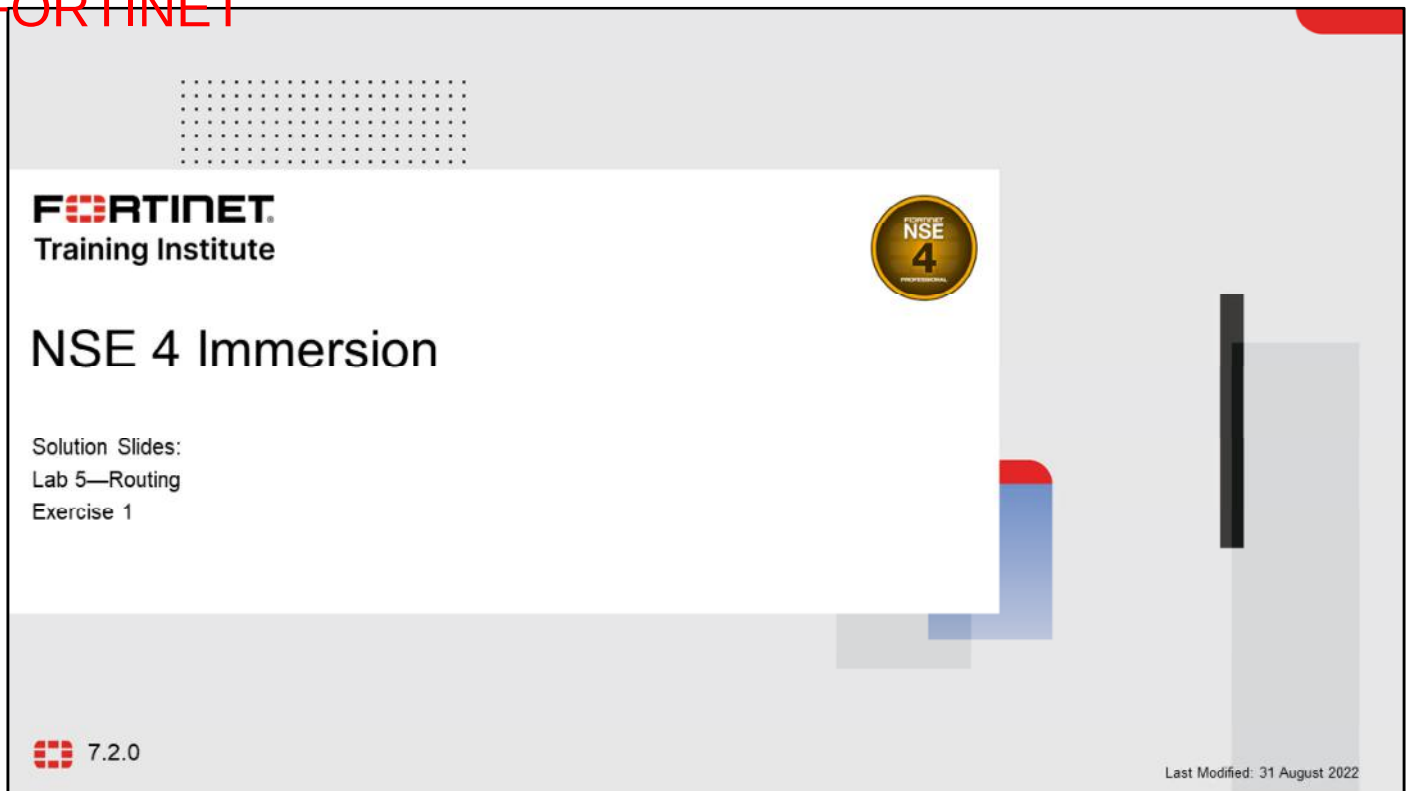
IPsec VPN—Firewall Policy—Remote

- Requirement:
 - Configure firewall policies for VPN traffic on Remote-FortiGate
- Solution:

Policy & Object > Firewall Policy

Name	Source	Destination	Schedule	Service	Action	NAT
port6 → port4	port6	port4				
port6 → ToLocal	port6	ToLocal				
Local_out	REMOTE_SUBNET	LOCAL_SUBNET	always	ALL	ACCEPT	Disabled
ToLocal → port6	ToLocal	port6				
Local_in	LOCAL_SUBNET	REMOTE_SUBNET	always	ALL	ACCEPT	Disabled

DO NOT REPRINT
© FORTINET



The slide features a light gray background with a white rectangular area on the left. At the top left of this white area is a grid of small dots. The Fortinet logo and 'Training Institute' text are positioned below the dots. To the right of the logo is a gold circular badge with 'NSE 4' and 'PROFESSIONAL' text. The main title 'NSE 4 Immersion' is centered in the white area. Below the title, the text 'Solution Slides:', 'Lab 5—Routing', and 'Exercise 1' is listed. In the bottom left corner of the slide, the Fortinet logo and '7.2.0' are displayed. In the bottom right corner, the text 'Last Modified: 31 August 2022' is shown. The slide is decorated with abstract geometric shapes in red, blue, and black.

FORTINET
Training Institute

NSE 4 Immersion

Solution Slides:
Lab 5—Routing
Exercise 1

7.2.0

Last Modified: 31 August 2022

These slides contain the solutions to the labs.

DO NOT REPRINT
© FORTINET

ECMP Routing—Backup Default Route

- Requirement:
 - Configure a second default route on Local-FortiGate
- Solution:

Network > Static Routes

New Static Route

Destination	Subnet Internet Service
	0.0.0.0/0.0.0.0
Gateway Address	10.200.2.254
Interface	port2
Administrative Distance	20
Comments	Write a comment... 0/255
Status	Enabled Disabled
Advanced Options	
Priority	5

DO NOT REPRINT
© FORTINET

ECMP Routing—Backup Default Route—Firewall Policy

- Requirement:
 - Configure a firewall policy for the second default route on Local-FortiGate
- Solution:

Policy & Object > Firewall Policy

New Policy

Name: Backup_Access

Incoming Interface: port3

Outgoing Interface: port2

Source: LOCAL_SUBNET

Destination: all

Schedule: always

Service: ALL

Action: ☒ ACCEPT ☐ DENY

Inspection Mode: ☒ Flow-based ☐ Proxy-based

Firewall / Network Options

NAT: ☒

Logging Options

Log Allowed Traffic: ☒ Security Events ☒ All Sessions

View the routing table and database

```
Local-FortiGate # get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       V - BGP VPNv4
       > - selected route, * - FIB route, p - stale info

Routing table for VRF=0
S   *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1, [1/0]
    *>      [10/0] via 10.200.2.254, port2, [5/0]
C   *> 10.0.1.0/24 is directly connected, port3
C   *> 10.200.1.0/24 is directly connected, port1
C   *> 10.200.2.0/24 is directly connected, port2
C   *> 172.16.100.0/24 is directly connected, port8
```

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

3

DO NOT REPRINT
© FORTINET

ECMP Routing—Link Health Monitor

- Requirement:
 - Configure link health monitor on Local-FortiGate
- Solution:

```
config system link-monitor
  edit port1-monitor
    set srcintf port1
    set server 4.2.2.1
    set gateway-ip 10.200.1.254
    set protocol ping
    set update-static-route enable
  next
  edit port2-monitor
    set srcintf port2
    set server 4.2.2.2
    set gateway-ip 10.200.2.254
    set protocol ping
    set update-static-route enable
end
```

DO NOT REPRINT
© FORTINET

ECMP Routing—Link Health Monitor

- Requirement:
 - Configure link health monitor to fail on port1 on Local-FortiGate
- Solution:

```
config system link-monitor
edit port1-monitor
set server 10.200.1.13
end
```

10.200.1.13 is a non-existent host in the lab network

Log & Report > System Events > General System Events

Date/Time	Level	User	Message	Log Description
20 minutes ago	INFO		FortiGate scheduled update fbi=yes fci=yes from 1001.241.8090	FortiGate update succeeded
34 minutes ago	WARNING		Static route on interface port1 may be removed by link-monitor port1-monitor.	Routing information changed
34 minutes ago	INFO		Static route is changed from 0 to 1	Link monitor status
34 minutes ago	INFO		Link Monitor initial state is dead, protocol: ping	Link monitor status
34 minutes ago	INFO	admin	Edit system-link-monitor port1-monitor	Object attribute configured
37 minutes ago	INFO	admin	Administrator admin logged in successfully from vsh(172.16.100.1)	Admin login successful
38 minutes ago	INFO	admin	Administrator admin logged out from vsh(172.16.100.1)	Admin logout successful
38 minutes ago	INFO	admin	Configuration is changed in the admin session	Configuration changed
38 minutes ago	INFO	admin	Administrator admin logged out from vsh(172.16.100.1)	Admin logout successful

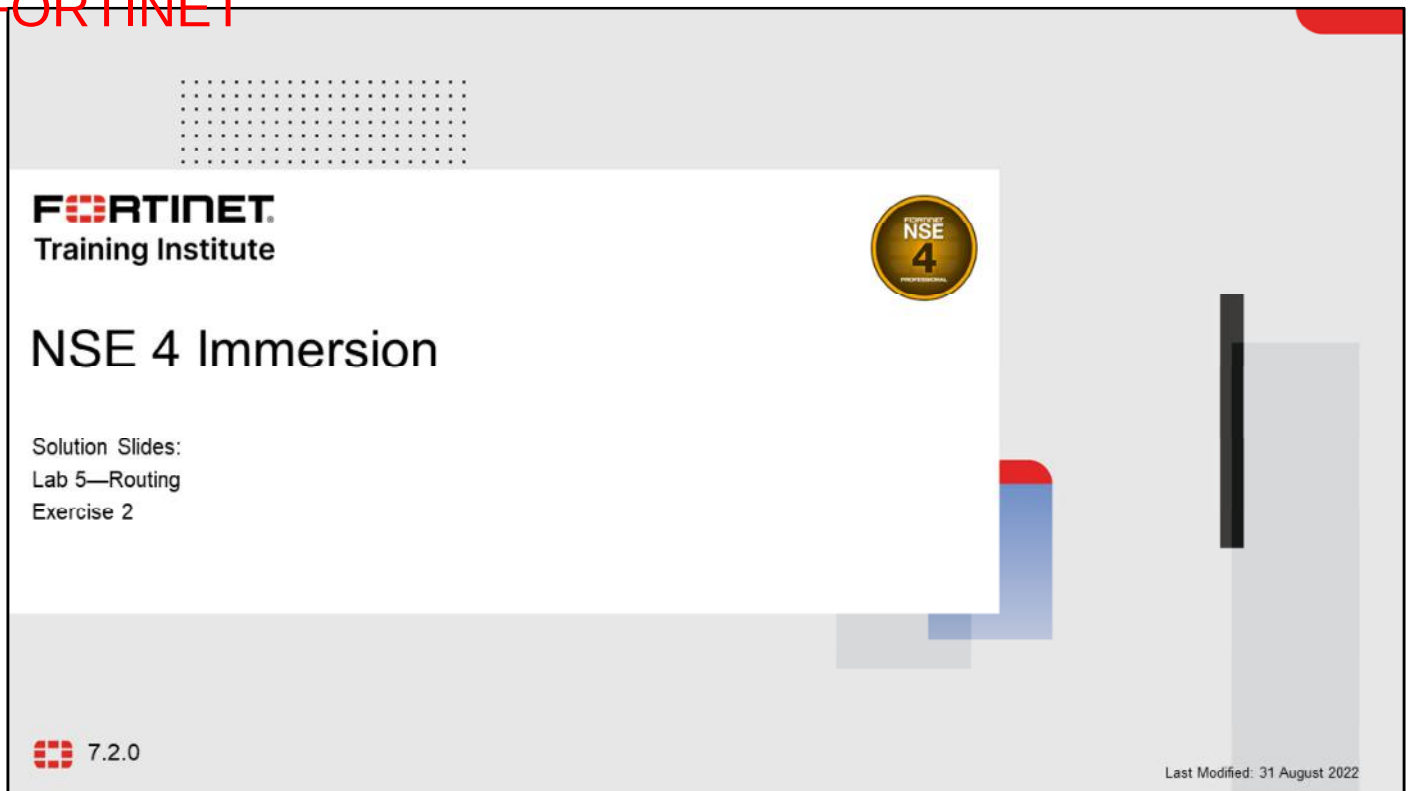
Log Details	
General	
Absolute Date/Time	2022/04/21 04:36:43
Time	04:36:43
Virtual Domain	root
Log Description	Routing information changed
Source	
Interface	port1
User	1 user
Action	
Status	down
Security	
Level	INFO
Event	
Message	Static route on interface port1 may be removed by link-monitor port1-monitor. Route: (10.200.1.1->10.200.1.13 ping-down)
Other	
Log event original timestamp	1650541003157495600
Timezone	-0700
Log ID	0100022921
Type	event
Sub Type	system
Name	port1-monitor

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

5

DO NOT REPRINT
© FORTINET



The slide features a light gray background with a white rectangular area on the left. In the top left corner of the white area is a grid of small dots. The Fortinet logo is positioned in the top left of the white area, with the text 'FORTINET' in bold and 'Training Institute' below it. To the right of the logo is a gold circular badge with 'NSE 4' and 'PROFESSIONAL' inside. The title 'NSE 4 Immersion' is centered in the white area. Below the title, the text 'Solution Slides:', 'Lab 5—Routing', and 'Exercise 2' is listed. In the bottom left corner of the white area is the Fortinet logo followed by '7.2.0'. In the bottom right corner of the slide, outside the white area, is the text 'Last Modified: 31 August 2022'. The slide is decorated with abstract geometric shapes: a red semi-circle in the top right, a blue and red L-shaped block in the bottom right, and a vertical black bar on the right side.

FORTINET
Training Institute

NSE 4 Immersion

Solution Slides:
Lab 5—Routing
Exercise 2

7.2.0

Last Modified: 31 August 2022

These slides contain the solutions to the labs.

DO NOT REPRINT
© FORTINET

ECMP Routing—ECMP Settings

- Requirement:
 - Configure ECMP load balancing method on Local-FortiGate
- Solution:

Network > Static Routes

Destination	Subnet	Internet Service
	0.0.0.0/0.0.0.0	
Gateway Address	10.200.1.254	
Interface	port1	
Administrative Distance	10	

Destination	Subnet	Internet Service
	0.0.0.0/0.0.0.0	
Gateway Address	10.200.2.254	
Interface	port2	
Administrative Distance	10	

```
config system settings
  set v4-ecmp-mode source-dest-ip-based
end
```

To set ECMP load balancing method based on source and destination IP address

Network > Static Routes

Advanced Options	
Priority	1

Change Priority value on the backup default route to match the primary default route

Exercise 2

Default priority value has changed to 1 from 0 in the latest FortiOS version.

ECMP Routing—ECMP Test

- Requirement:
 - Configure packet capture and review routing table
- Solution:

```
Local-FortiGate # get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, Ia - IS-IS inter area
V - BGP Vpnv4
> - selected route, * - FIB route, p - stale info

Routing table for VRF-0
S * 0.0.0.0/0 [10/0] via 10.200.1.254, port1, [1/0]
S * 0.0.0.0/0 [10/0] via 10.200.2.254, port2, [1/0]
C * 10.200.1.0/24 is directly connected, port1
C * 10.200.2.0/24 is directly connected, port2
C * 172.16.100.0/24 is directly connected, port8
```

Both default routes
should be up and active

The SYN packets
are egressing both
port1 and port2

```
Local-FortiGate # diagnose sniffer packet any 'tcp[13]&2==2 and port 80' 4
Using Original Sniffing Mode
interfaces=[any]
filters=[tcp[13]&2==2 and port 80]
33.859379 port3 in 10.0.1.10.45520 -> 172.217.0.35.80: syn 240590500
33.859441 port2 out 10.200.2.1.45520 -> 172.217.0.35.80: syn 240590500
33.860738 port2 in 172.217.0.35.80 -> 10.200.2.1.45520: syn 3841123407 ack 2
0501
33.860776 port3 out 172.217.0.35.80 -> 10.0.1.10.45520: syn 3841123407 ack 2
0501
34.120934 port3 in 10.0.1.10.33914 -> 13.32.196.214.80: syn 907850234
34.120981 port1 out 10.200.1.1.33914 -> 13.32.196.214.80: syn 907850234
34.121135 port3 in 10.0.1.10.33916 -> 13.32.196.214.80: syn 726691258
34.121168 port1 out 10.200.1.1.33916 -> 13.32.196.214.80: syn 726691258
34.123351 port1 in 13.32.196.214.80 -> 10.200.1.1.33914: syn 642315855 ack 9
0235
34.123369 port3 out 13.32.196.214.80 -> 10.0.1.10.33914: syn 642315855 ack 9
0235
```

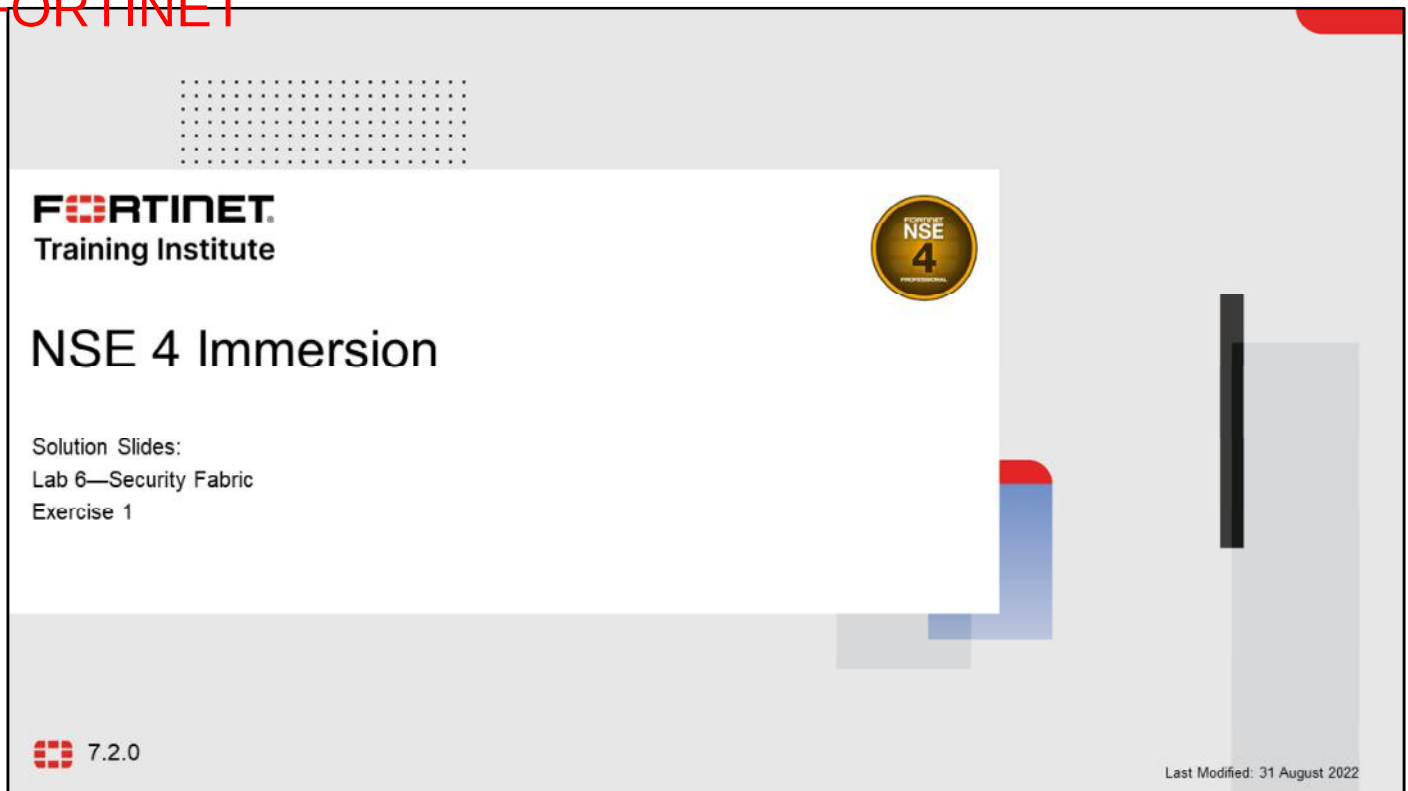
FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

3

You may need to clear sessions on FortiGate to see desired result on packet capture. The CLI command `diagnose system session clear` can be used to clear sessions. Note that this command clears all the current session on the FortiGate.

DO NOT REPRINT
© FORTINET

The slide features a light gray background with a white rectangular area on the left. At the top left of this white area is a grid of small dots. The Fortinet logo and 'Training Institute' text are positioned below the dots. To the right of the logo is a gold circular badge with 'NSE 4' and 'PROFESSIONAL' text. The main title 'NSE 4 Immersion' is centered in the white area. Below the title, the text 'Solution Slides:', 'Lab 6—Security Fabric', and 'Exercise 1' are listed. In the bottom left corner of the slide, the Fortinet logo and '7.2.0' are displayed. In the bottom right corner, the text 'Last Modified: 31 August 2022' is present. The slide is decorated with abstract geometric shapes in red and blue on the right side.

FORTINET
Training Institute

NSE 4
PROFESSIONAL

NSE 4 Immersion

Solution Slides:
Lab 6—Security Fabric
Exercise 1

7.2.0

Last Modified: 31 August 2022

These slides contain the solutions to the labs.

DO NOT REPRINT
© FORTINET

Security Fabric—Local-FortiGate (Root) Device

- Requirement:
 - You must enable Security Fabric on the root FortiGate
- Solution:

Network > Interfaces

Edit Interface

Administrative Access

IPv4

☒ HTTPS	☒ HTTP	☒ PING
☐ FMG-Access	☒ SSH	☐ SNMP
☒ TELNET	☐ FTM	☐ RADIUS Accounting
☒ Security Fabric Connection	☐ Speed Test	

Receive LLDP *i* Use VDOM Setting Enable Disable

Transmit LLDP *i* Use VDOM Setting Enable Disable

☐ DHCP Server

Network

Device detection *i* ☒

Security Fabric > Fabric Connectors

FortiAnalyzer Settings

Status: ☒ Enabled ☐ Disabled

IP address: 10.0.1.210 Test Connectivity

Connection status: ☐ Unauthenticated

Upload option: *i* Real Time Every Minute Every 5 Minutes

Allow access to FortiGate REST API: ☒

Verify FortiAnalyzer certificate: ☒

Security Fabric Settings

Status: ☒ Enabled ☐ Disabled

Security Fabric role: ☒ Serve as Fabric Root Join Existing Fabric

Fabric name: fortinet

Allow other Security Fabric devices to join: ☒

Device authorization: None Edit

Allow downstream device REST API access: *i* ☐

SAML Single Sign-On: *i* ☐ Advanced Options

Management IP/FQDN: *i* ☐ Use WAN IP Specify

Management port: ☒ Use Admin Port Specify

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

2

You will configure the Security Fabric tree, starting with the root device (Local-FortiGate).

1. Enable **Security Fabric Connection** and **Device detection** on the **port3** network interface settings.
2. Configure the FortiAnalyzer IP address on the **FortiAnalyzer Logging** in **Fabric Connectors**.
3. Enable Security Fabric in **Fabric Connectors**. You must set the role to **Serve as Fabric Root** and then set the fabric name as `fortinet`.
4. The root device must allow other security fabric devices on the **port3** and **To-Remote-HQ2** interfaces.

Security Fabric—ISFW (Leaf) Device

- Requirement:
 - You must enable Security Fabric on leaf devices
- Solution:

Network > Interfaces

Administrative Access

IPv4

☒ HTTPS ☒ HTTP ☒ PING

☐ FMG-Access ☒ SSH ☐ SNMP

☐ FTM ☐ RADIUS Accounting ☒ Security Fabric Connection

☐ Speed Test

Receive LLDP ☒ Use VDOM Setting: Enable Disable

Transmit LLDP ☒ Use VDOM Setting: Enable Disable

☐ DHCP Server

Network

Device detection ☒

Security Fabric > Fabric Connectors

Security Fabric Connector

Security Fabric Settings

Status: ☒ Enabled ☐ Disabled

Security Fabric role:

Upstream FortiGate IP: 10.0.1.254

Allow other Security Fabric devices to join: ☒ port1 port3

Allow downstream device REST API access: ☒

SAML Single Sign-On:

Mode: Pending

Default login page: super_admin

Default admin profile:

Management IP/FQDN: 10.0.1.200

Management port:

(root) Security Fabric > Fabric Connectors

Topology

Please authorize the highlighted devices below.

Local-FortiGate (Fabric Root)

☒ Show in Security Fabric > Security Rating

☒ Login to FGVM010000077646

1. Enable **Security Fabric Connection** and **Device detection** on the **port1** and **port3** network interface settings.
2. Enable Security Fabric in **Fabric Connectors**. You must set the role to **Join Existing Fabric** and use root FortiGate IP address, 10.0.1.254.
3. Select **super_admin** in **Default admin profile** field.
4. Authorize ISFW on the root FortiGate Fabric in **Fabric Connectors**, in the **Topology** section on the right.

Check the Security Fabric deployment result on the root Local-FortiGate in **Dashboard > Status** within **Security Fabric widget**. Also, check the result in **Security Fabric > Physical Topology** and **Logical Topology**.

DO NOT REPRINT
© FORTINET

Security Fabric—Remote-FortiGate (Leaf) Device

- Requirement:
 - You must enable Security Fabric on leaf devices
- Solution:

Network > Interfaces

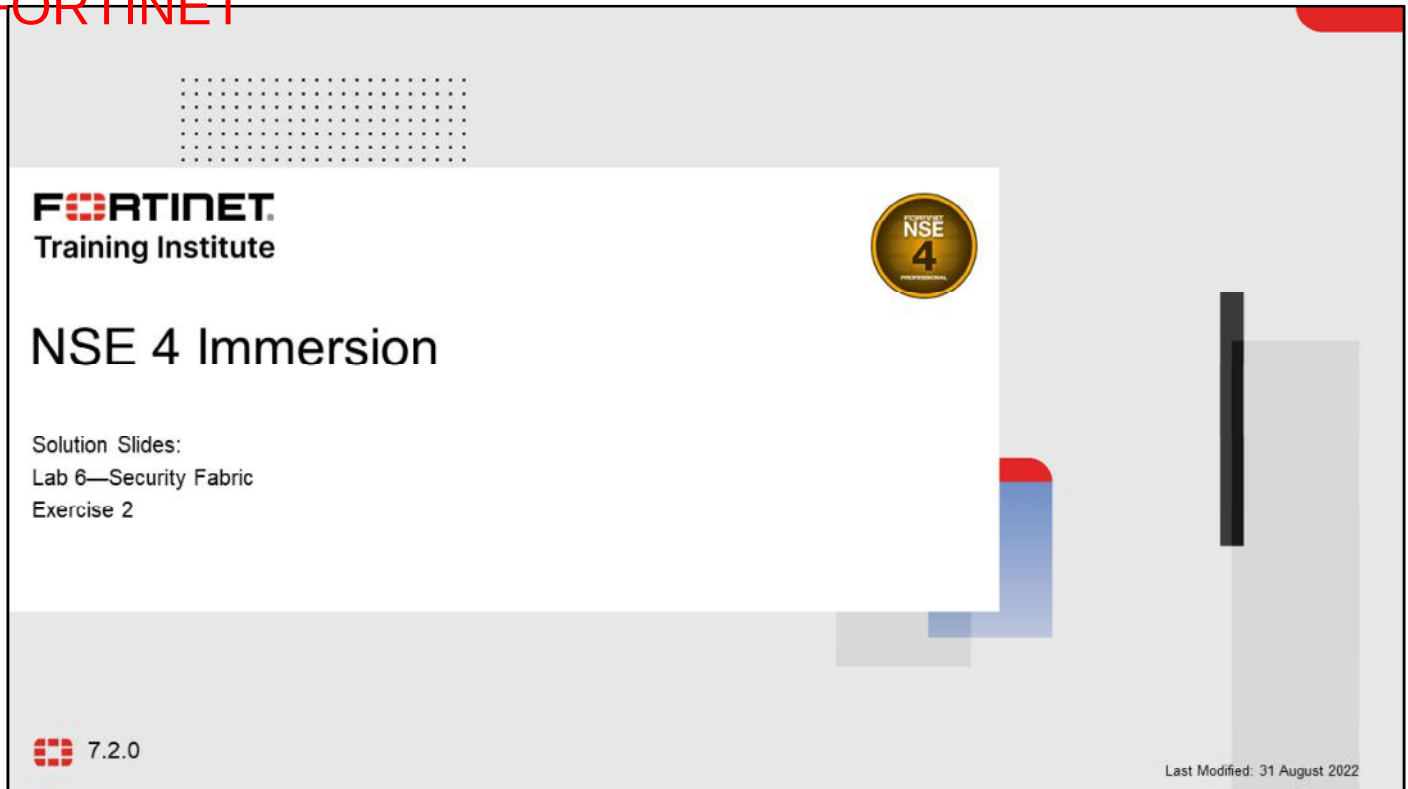
(root) Security Fabric > Fabric Connectors

Security Fabric > Fabric Connectors

1. Enable **Security Fabric Connection** and **Device detection** on the **port6** and **To-Local-HQ1** network interface settings.
2. Enable Security Fabric in **Fabric Connectors**. You must set the role to **Join Existing Fabric** and use the root FortiGate IP address, 10.10.10.1.
3. Select **super_admin** in **Default admin profile** field.
4. Authorize **Remote-FortiGate** on the root FortiGate Fabric in **Fabric Connectors**, in the **Topology** section on the right.

Check the Security Fabric deployment result on the root Local-FortiGate in **Dashboard > Status** within **Security Fabric widget**. Also, check the result in **Security Fabric > Physical Topology** and **Logical Topology**.

DO NOT REPRINT
© FORTINET



The slide is a presentation slide for Fortinet Training Institute. It features a white background with a grey border. In the top left corner, there is a grid of small dots. The Fortinet logo is in the top left, followed by "Training Institute". A gold circular badge with "NSE 4" is in the top right. The title "NSE 4 Immersion" is in the center. Below it, the text "Solution Slides:", "Lab 6—Security Fabric", and "Exercise 2" is listed. In the bottom left, there is a red logo and "7.2.0". In the bottom right, it says "Last Modified: 31 August 2022".

FORTINET
Training Institute

NSE 4 Immersion

Solution Slides:
Lab 6—Security Fabric
Exercise 2

7.2.0

Last Modified: 31 August 2022

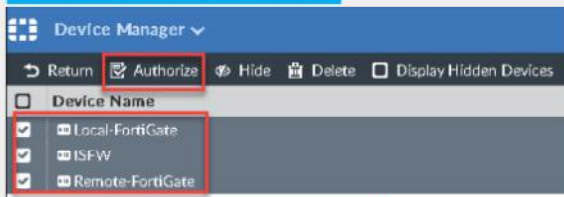
These slides contain the solutions to the labs.

DO NOT REPRINT
© FORTINET

Security Fabric—FortiAnalyzer

- Requirement:
 - You must authorize Security Fabric devices on FortiAnalyzer
- Solution:

Device Manager > Unauthorized

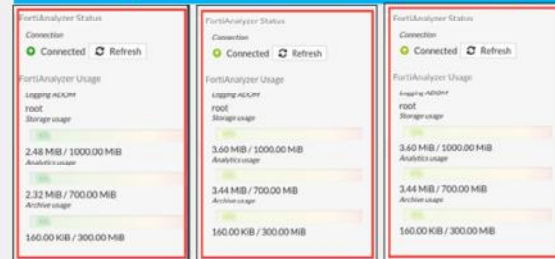


3 Devices Total			0 Devices Unauthorized
Device Name	IP Address	Platform	Logs
ISFW	10.0.1.300	FortiGate-VM64	Real Time
Local-FortiGate	10.0.1.254	FortiGate-VM64	Real Time
Remote-FortiGate	10.0.1.254	FortiGate-VM64	Real Time

Security Fabric > Logical Topology



Security Fabric > Fabric Connectors > FortiAnalyzer Logging



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

2

- Log in to FortiAnalyzer to authorize Security Fabric devices.
- Click **Device Manager > Unauthorized**.
- Select all devices, and then click **Authorize**. The logs status should be green for all devices.

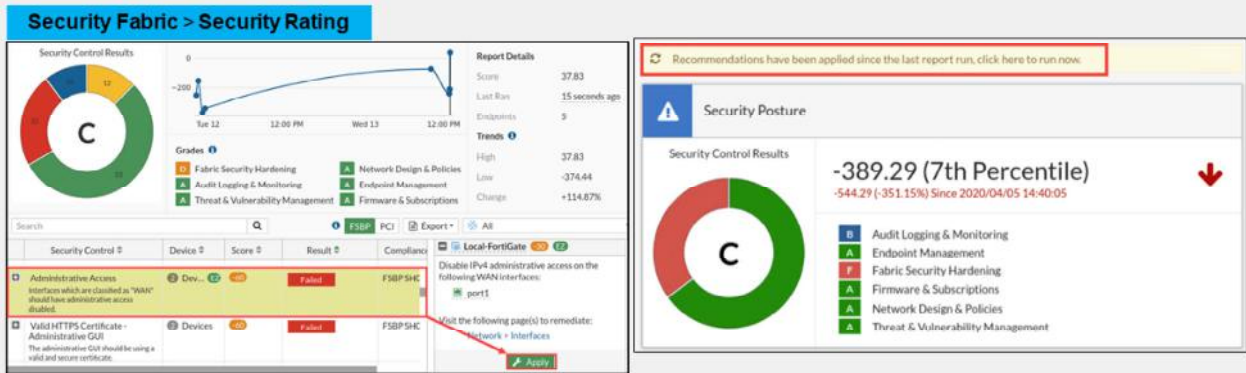
You can review FortiAnalyzer logging status on all devices at **Security Fabric > Fabric Connectors > FortiAnalyzer Logging**.

You can review the Security Fabric logical topology to verify the setup is complete.

DO NOT REPRINT
© FORTINET

Security Fabric—Security Ratings

- Requirement:
 - You must apply security ratings recommendations
- Solution:



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

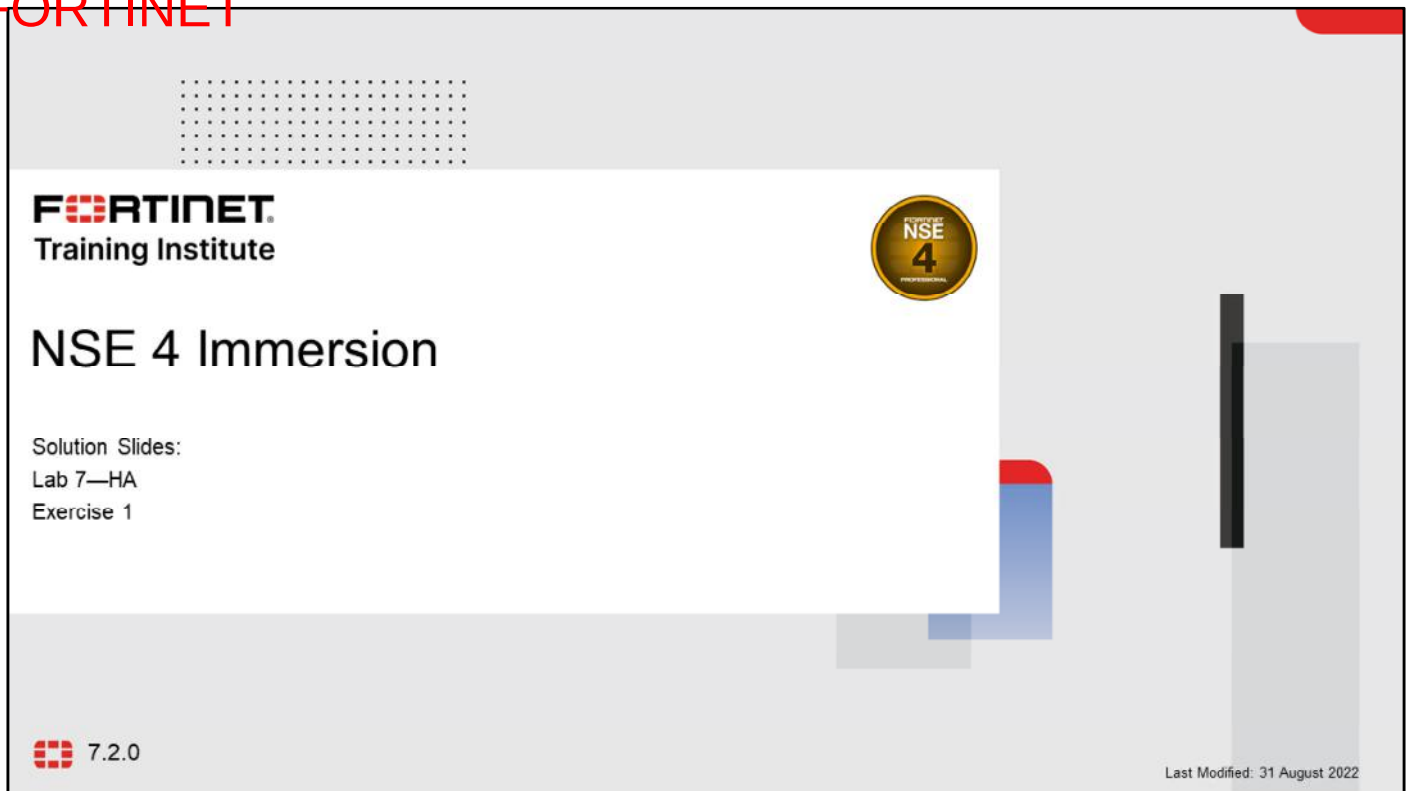
3

The security rating feature includes three major score cards: **Security Posture**, **Fabric Coverage**, and **Optimization**.

1. In **Security Fabric > Security Rating**, click **Security Posture** to show the scorecard details.
2. In the **Security Control** column, select or search **Audit Log Settings**.
3. On the pane on the right, in the **Local-FortiGate** section, click **Apply**.
4. The **View Diff** button will appear next to **Apply** after you successfully apply audit log settings.

Run the report again by navigating again to **Security Fabric > Security Rating**. Click **Run Now** to get the new security posture score.

DO NOT REPRINT
© FORTINET

A presentation slide with a light gray background. At the top left, there is a grid of small dots. Below it, the Fortinet logo and 'Training Institute' are displayed. To the right of the logo is a gold circular badge with 'NSE 4' and 'PROFESSIONAL' text. The main title 'NSE 4 Immersion' is in large black font. Below the title, it says 'Solution Slides:', 'Lab 7—HA', and 'Exercise 1'. In the bottom left corner, there is a red square icon followed by '7.2.0'. In the bottom right corner, it says 'Last Modified: 31 August 2022'.

FORTINET
Training Institute

NSE 4
PROFESSIONAL

NSE 4 Immersion

Solution Slides:
Lab 7—HA
Exercise 1

7.2.0

Last Modified: 31 August 2022

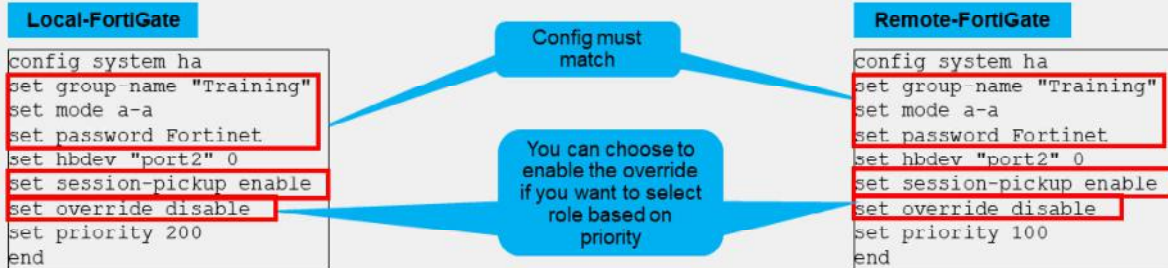
These slides contain the solutions to the labs.

DO NOT REPRINT

© FORTINET

HA Setup

- Requirement:
 - Set up an active-active HA cluster between Local-FortiGate and Remote-FortiGate with heartbeat interface port2 on both FortiGate devices
 - Local-FortiGate must be the primary device
 - Session pickup must be enabled
- Solution:
 - You can configure HA from either GUI or CLI



You can configure FortiGate devices using the CLI to form an HA cluster. To select the primary device, you have two options:

- If override is disabled, FortiGate checks the uptime of the device first and selects the device with the largest uptime. If the uptime for both the devices is within a five-minute range, the FortiGate device with the higher priority is selected as the primary device.
- If override is enabled, Fortigate checks priority before uptime. The Fortigate device with the highest priority is selected as the primary device.

DO NOT REPRINT
© FORTINET

HA Setup (Contd)

- Solution:
 - From GUI:

Local-FortiGate

System > HA

High Availability

Mode: **Active-Active**

Device priority: 200

Cluster Settings

Group name: **Training**

Password: **Fortinet**

Session pickup: ☒

Monitor interfaces: +

Heartbeat interfaces: **port2** +

☐ Management Interface Reservation

Remote-FortiGate

System > HA

High Availability

Mode: **Active-Active**

Device priority: 100

Cluster Settings

Group name: **Training**

Password: **Fortinet**

Session pickup: ☐

Monitor interfaces: +

Heartbeat interfaces: **port2** +

☐ Management Interface Reservation

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

3

DO NOT REPRINT
© FORTINET

Syncing Configuration

- Requirement:
 - Configuration must be in sync
- Solution:
 - After configuring HA, the configuration will automatically sync. You do not need to take any extra steps to sync the configuration between FortiGate devices

DO NOT REPRINT
© FORTINET

Testing

```
Local-FortiGate # diagnose sys ha checksum cluster
===== FGVM010000064692 =====
is_manage_primary()=1, is_root_primary()=1
debugzone
global: 3a 90 6b 13 f9 5b 95 19 85 f0 64 bc d1 58 e6 17
root: 21 40 e3 25 43 89 d4 ba 6c d7 d6 4f ed b8 d0 21
all: 8d fd a7 46 dd eb c2 51 e0 c0 f3 10 0d d1 0c ec
checksum
global: 3a 90 6b 13 f9 5b 95 19 85 f0 64 bc d1 58 e6 17
root: 21 40 e3 25 43 89 d4 ba 6c d7 d6 4f ed b8 d0 21
all: 8d fd a7 46 dd eb c2 51 e0 c0 f3 10 0d d1 0c ec

===== FGVM010000065036 =====
is_manage_primary()=0, is_root_primary()=0
debugzone
global: 3a 90 6b 13 f9 5b 95 19 85 f0 64 bc d1 58 e6 17
root: 21 40 e3 25 43 89 d4 ba 6c d7 d6 4f ed b8 d0 21
all: 8d fd a7 46 dd eb c2 51 e0 c0 f3 10 0d d1 0c ec
checksum
global: 3a 90 6b 13 f9 5b 95 19 85 f0 64 bc d1 58 e6 17
root: 21 40 e3 25 43 89 d4 ba 6c d7 d6 4f ed b8 d0 21
all: 8d fd a7 46 dd eb c2 51 e0 c0 f3 10 0d d1 0c ec
```

```
Local-FortiGate #get sys status
Firmware Signature:
certified7.2.0,build1157,220331 (GA.F)

Virus-DB: 89.05692(2021-10-06 11:26)
Extended DB: 89.05692(2021-10-06 11:25)
Extreme DB: 1.00000(2018-04-09 18:07)
IPS-DB: 6.00741(2015-12-01 02:30)6 11:45)

.....
Current HA mode: a-a, primary
Cluster state change time: 2022-04-25
03:39:55

Branch point: 1157
Release Version Information: GA
FortiOS x86-64: Yes
Last reboot reason: warm reboot1 2022
```

Checksum must match for
both FortiGate devices

The checksum value shown on the slide may differ from your output.

DO NOT REPRINT
© FORTINET

Testing (Contd)

```
Local-FortiGate # get system ha status
HA Health Status: OK
Model: FortiGate-VM64-KVM
Mode: HA A-A
Group: 0
Debug: 0
Cluster Uptime: 0 days 0:12:56
Cluster state change time: 2022-04-25 03:39:55
Primary selected using:
  <2022/04/25 03:39:55> vcluster-1: FGVM010000064692 is selected as the primary because its override
priority is larger than peer member FGVM010000065036.
  <2022/04/25 03:38:07> vcluster-1: FGVM010000064692 is selected as the primary because it's the only
member in the cluster.
ses_pickup: enable, ses_pickup_delay=disable
load_balance: disable
load_balance_udp: disable
schedule: Round robin.
upgrade_mode: unset
override: disable
Configuration Status:
  FGVM010000064692(updated 1 seconds ago): in-sync
  FGVM010000065036(updated 4 seconds ago): in-sync
```

DO NOT REPRINT
© FORTINET

Failover

- Requirement:
 - Trigger an HA failover to make sure the traffic fails over to the backup FortiGate
- Solution:
 - You have three options to test failover:
 - If override is enabled, you can change the priority of Local-FortiGate and set it lower than 100
 - If override is disabled, you can reset the uptime on the Local-FortiGate using the command `diagnose sys ha reset-uptime`
 - You can also choose to reboot Local-FortiGate to force failover regardless of the configuration

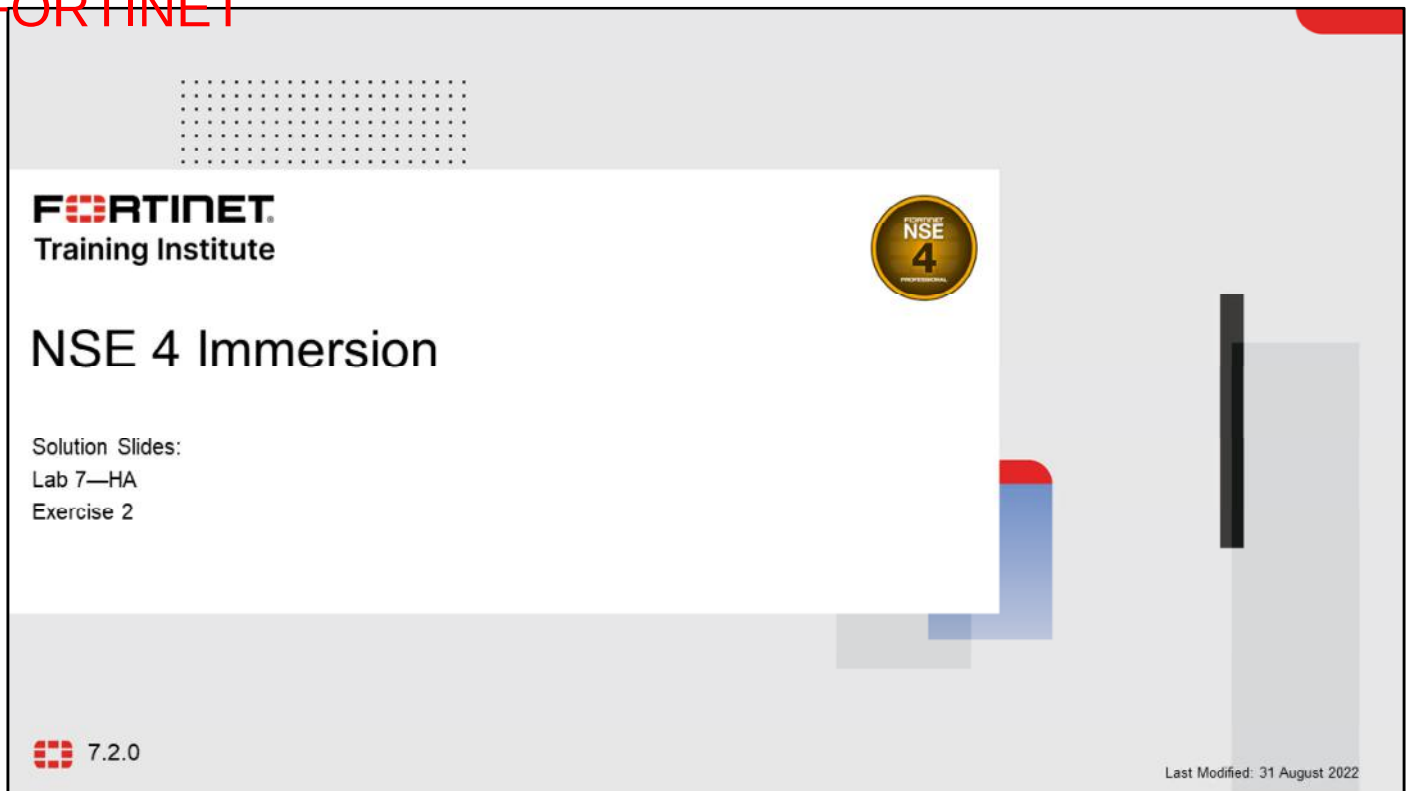
Testing Failover

- Start a ping on Local-Client to 8.8.8.8
- Reboot Local-FortiGate
- Reconnect to the HA cluster using the same IP
- Run command `get system status`

```
Remote-FortiGate # get sys status
Version: FortiGate-VM64-KVM v7.2.0,build1157,220331 (GA.F)
Firmware Signature: certified
Serial-Number: FGVM010000065036
Hostname: Remote-FortiGate
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: a-a, primary
Cluster uptime: 45 minutes, 58 seconds
Cluster state change time: 2022-04-25 03:55:51
Branch point: 1157
Release Version Information: GA
FortiOS x86-64: Yes
System time: Mon Apr 25 03:56:15 2022
```

```
Administrator@ubuntu-1804-desktop:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:
64 bytes from 8.8.8.8: icmp_seq=1 ttl=112 time=2.36 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=112 time=1.46 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=112 time=1.35 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=112 time=1.81 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=112 time=1.73 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=112 time=1.70 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=112 time=1.57 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=112 time=1.49 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=112 time=1.44 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=112 time=1.36 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=112 time=1.52 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=112 time=1.48 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=112 time=1.85 ms
64 bytes from 8.8.8.8: icmp_seq=14 ttl=112 time=1.55 ms
64 bytes from 8.8.8.8: icmp_seq=15 ttl=112 time=1.53 ms
64 bytes from 8.8.8.8: icmp_seq=16 ttl=112 time=1.81 ms
64 bytes from 8.8.8.8: icmp_seq=17 ttl=112 time=1.38 ms
64 bytes from 8.8.8.8: icmp_seq=18 ttl=112 time=1.56 ms
64 bytes from 8.8.8.8: icmp_seq=19 ttl=112 time=1.52 ms
64 bytes from 8.8.8.8: icmp_seq=20 ttl=112 time=1.50 ms
64 bytes from 8.8.8.8: icmp_seq=21 ttl=112 time=1.57 ms
64 bytes from 8.8.8.8: icmp_seq=22 ttl=112 time=1.34 ms
64 bytes from 8.8.8.8: icmp_seq=23 ttl=112 time=1.46 ms
64 bytes from 8.8.8.8: icmp_seq=24 ttl=112 time=1.54 ms
64 bytes from 8.8.8.8: icmp_seq=25 ttl=112 time=1.52 ms
64 bytes from 8.8.8.8: icmp_seq=26 ttl=112 time=1.44 ms
64 bytes from 8.8.8.8: icmp_seq=27 ttl=112 time=1.57 ms
64 bytes from 8.8.8.8: icmp_seq=28 ttl=112 time=1.53 ms
64 bytes from 8.8.8.8: icmp_seq=29 ttl=112 time=2.06 ms
64 bytes from 8.8.8.8: icmp_seq=30 ttl=112 time=1.52 ms
```

DO NOT REPRINT
© FORTINET



The slide features a light gray background with a white rectangular area on the left. At the top left of this white area is a grid of small dots. Below the grid is the Fortinet logo and the text 'Training Institute'. To the right of the logo is a gold circular badge with 'NSE 4' and 'PROFESSIONAL' text. Below the logo and badge is the title 'NSE 4 Immersion'. Further down is the text 'Solution Slides:', 'Lab 7—HA', and 'Exercise 2'. At the bottom left of the white area is the Fortinet logo and '7.2.0'. At the bottom right of the slide is the text 'Last Modified: 31 August 2022'. The slide is decorated with various geometric shapes: a red semi-circle at the top right, a blue and red L-shaped block, and a black vertical bar.

FORTINET
Training Institute

NSE 4 Immersion

Solution Slides:
Lab 7—HA
Exercise 2

7.2.0

Last Modified: 31 August 2022

These slides contain the solutions to the labs.

DO NOT REPRINT
© FORTINET

HA Management Interface

- Requirement:
 - Configure the HA management interface
- Solution:
 - Access the secondary FortiGate from the primary FortiGate CLI:

```
Remote-FortiGate # execute ha manage 1 admin
Warning: Permanently added '169.254.0.2' (ED25519) to the list of known hosts.
admin@169.254.0.2's password:
Local-FortiGate #
```

You can configure the HA management interface using the GUI or CLI. To access the secondary FortiGate from the primary FortiGate CLI:

1. On the Remote-FortiGate CLI, log in with the username `admin` and password `password`.
2. Enter the following command to access the secondary FortiGate CLI through the primary FortiGate HA link: `execute ha manage <id> <admin_username>`

DO NOT REPRINT
© FORTINET

HA Management Interface

- Check the current HA status of the secondary FortiGate:

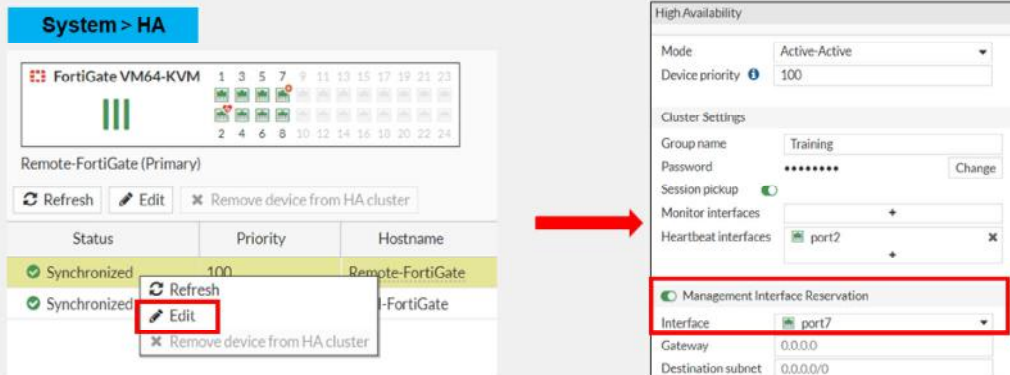
```
Local-FortiGate # get system status
Version: FortiGate-VM64-KVM v7.2.0,build1157,220331 (GA.F)
Firmware Signature: certified
Serial-Number: FGVM010000064692
License Status: Valid
VM Resources: 1 CPU/1 allowed, 2007 MB RAM
Log hard disk: Available
Hostname: Local-FortiGate
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Current HA mode: a-a, secondary
Cluster uptime: 28 minutes, 53 seconds
Cluster state change time: 2022-04-25 03:55:50
Branch point: 1157
Release Version Information: GA
FortiOS x86-64: Yes
System time: Mon Apr 25 04:06:40 2022
Last reboot reason: warm reboot
```

1. Enter the following command to get the status of the secondary FortiGate: `get system status` to view Current HA mode. You will notice that Remote-FortiGate is a-a secondary.
2. Run `exit` to return to the Remote-FortiGate CLI.

DO NOT REPRINT
© FORTINET

Set Up the Management Interface

- Requirement:
 - Assign port7 for the management interface reservation
- Solution



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

4

1. On the Local-Client VM, open a browser, and then log in to the Remote-FortiGate GUI (because this is a primary device) at 10.0.1.254 with the username `admin` and password `password`.
2. Click **System > HA**.
3. Right-click **Remote-FortiGate**, and then click **Edit**.
4. Enable **Management Interface Reservation**, and in the **Interface** field, select **port7**.

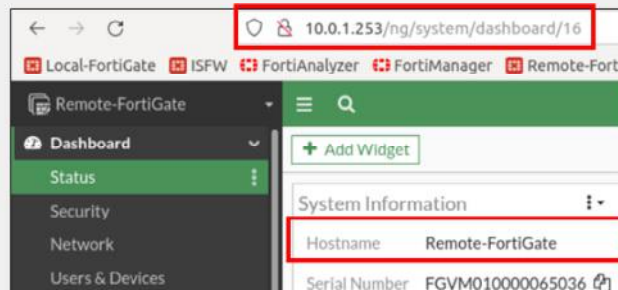
DO NOT REPRINT
© FORTINET

Set Up the HA Management (Contd)

- Requirement:
 - Configure and verify access to the primary FortiGate using the management interface

- Solution:

```
config system interface
edit port7
set ip 10.0.1.253/24
set allowaccess http snmp ping ssh
end
```



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

5

1. On the Remote-FortiGate CLI, log in with the username `admin` and password `password`.
2. Run the following commands to configure port7:


```
config system interface
edit port7
set ip 10.0.1.253/24
set allowaccess http snmp ping ssh
End
```
3. On the Local-Client VM, open a browser, and log in to the Remote-FortiGate GUI at 10.0.1.253 (note the IP address) with the username `admin` and password `password`. This verifies connectivity to port7.

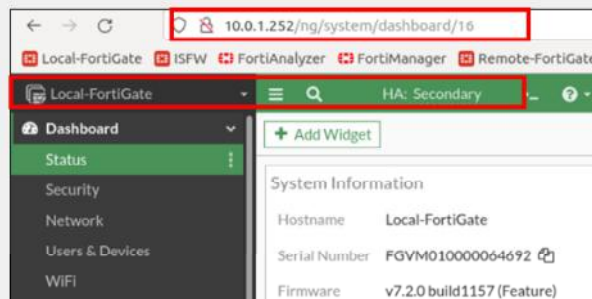
Set Up the HA Management (Contd)

- Configure and verify access to the secondary FortiGate using the management interface

```
Remote-FortiGate # execute ha manage 1 admin
admin@169.254.0.2's password:
Local-FortiGate # show system ha
config system ha
    set group-name "Training"
    set mode a-a
    set password ENC
ELxZPJHSBoZHW6yWt49DDv9jIEnYWwUN7FM8aVoqBICU+
/3ryAESwewIbhP5eDqNBF1Q==
    set hbdev "port2" 0
    set session-pickup enable
    set ha-mgmt-status enable
    config ha-mgmt-interfaces
        edit 1
            set interface "port7"
        next
    end
    set override disable
    set priority 200
end
```

- Configure port7 on the secondary FortiGate

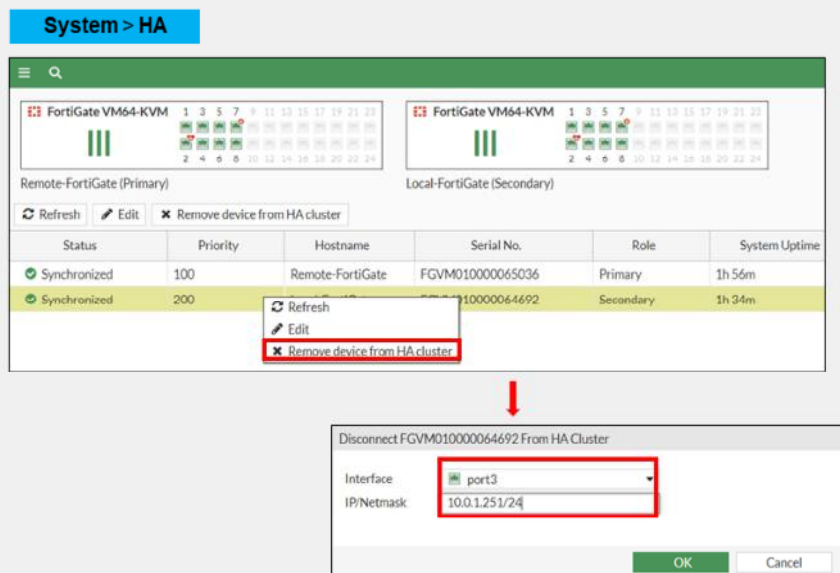
```
#show system interface
#config system interface
edit port7
set ip 10.0.1.252/24
set allowaccess http ping ssh snmp
end
```



- On the Remote-FortiGate CLI, enter the following command to verify HA configuration: `show system ha`.
- Look for `ha-mgmt-status` and `config ha-mgmt-interfaces`. These should already be set.
- Enter the following command to verify that port7 has no configuration:
`show system interface`
- Configure port7, as shown on this slide.
- On the Local-Client VM, open a browser, and then log in to the Local-FortiGate GUI at 10.0.1.252 (note the IP address) with the username `admin` and password `password`. This will verify connectivity to port7. Each device in the cluster now has its own management IP address for monitoring purposes.

DO NOT REPRINT
© FORTINET

Disconnect Secondary FortiGate From Cluster



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

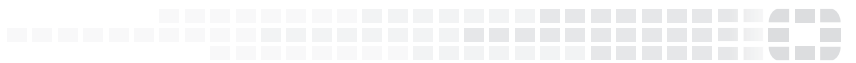
7

1. On the Local-Client VM, open a browser, and then log in to the Remote-FortiGate GUI at 10.0.1.254 with the username `admin` and password `password`.
2. Click **System > HA**.
3. Right-click **Local-FortiGate**, and then click **Remove device from HA cluster**. When prompted, configure the **Interface** and **IP/Network** settings.
4. Click **OK**.
5. On the Local-Client VM, open a browser, and then log in to the Local-FortiGate GUI at 10.0.1.251 (note the IP address) with the username `admin` and password `password`. This will verify connectivity to port3.

DO NOT REPRINT
© FORTINET



FORTINET®



No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Fortinet Inc., as stipulated by the United States Copyright Act of 1976.

Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.